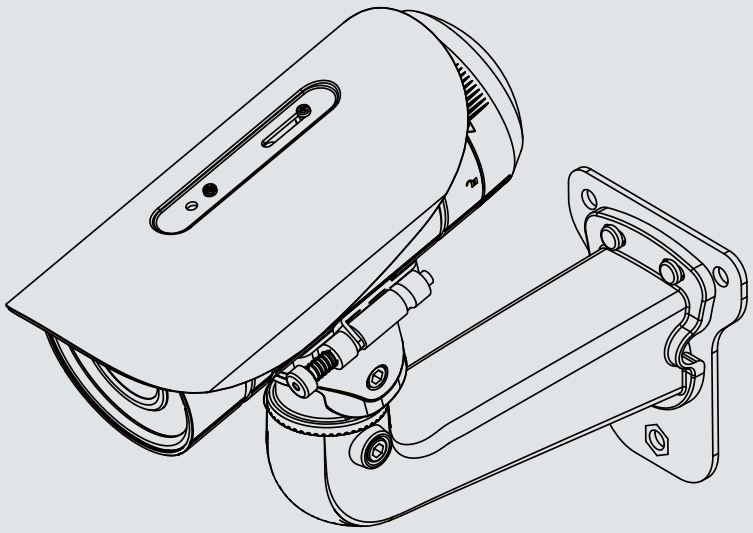
IP8355(E)H / IP8365(E)H

Bullet Network Camera

User's Manual

1.3 / 2MP • 30M IR • Smart Focus System • IP67 •
Cable Management



Rev. 1.3

Table of Contents

Overview 4
Revision History 4
Read Before Use 5
1. Package Contents 5
Symbols and Statements in this Document 5
2. Physical Description 6
3. Hardware Installation 7
4. Cabling Assembly 8
5. Network Deployment 11
Software Installation 17
Ready to Use 18
Accessing the Network Camera 20
Using Web Browsers 20
Using RTSP Players 23
Using 3GPP-compatible Mobile Devices 24
Using VIVOTEK Recording Software 25
Main Page 26
Client Settings 31
Configuration 35
System > General settings 36
System > Homepage layout 38
System > Logs 41
System > Parameters 43
System > Maintenance 44
Media > Image 48
Media > Video 58
Media > Audio 62
Network > General settings 63
Network > Streaming protocols 71
Network > SNMP (Simple Network Management Protocol) 80
Security > User Account 81
Security > HTTPS (Hypertext Transfer Protocol over SSL) 82
Security > Access List 89
PTZ > PTZ settings 94
Event > Event settings 98
Applications > Motion detection 112
Applications > DI and DO 115
Applications > Tampering detection 115
Applications > Audio detection 116
Applications > VADP (VIVOTEK Application Development Platform) 118
Recording > Recording settings 120
Local storage > SD card management 125
Local storage > Content management 126
Appendix 129

URL Commands for the Network Camera 129
Technical Specifications 213
Technology License Notice 215
Electromagnetic Compatibility (EMC) 216

Overview

VIVOTEK IP8355(E)H is a professional outdoor dome network camera offering 30 fps @ 1.3-Megapixel resolutions with superb image quality.

The IP8365(E)H provides up to 60 fps @ 2-Megapixel resolution with superb image quality.

Featuring the new improved Wide Dynamic Range Technology WDR Pro II [WDR Pro for IP8365(E)H], it provides extreme visibility in extremely dark & light environments with 4-shutter capture method. Combined with 3D Noise Reduction Technology, which enables the IP8355(E)H/IP8365(E)H to capture clear, polished video under low-light conditions and reduce bandwidth from sensor noise, users can identify an increased level of image detail in extremely bright as well as dark environments.

Additionally, as a professional day/night camera, the camera adopts a Smart IR technology which prevents overexposure and provides noise reduction to adjust the IR lighting intensity instantaneously based on the changes of light in the ambient environment.

To provide top-notch image quality, the camera also comes with a P-iris lens, which controls the iris with extreme precision with its built-in stepper motor. By using software controls, the lens maintains the iris opening at an optimal level at all times, resulting in superior sharpness and depth of field as well as image quality. Furthermore, for installers, properly adjusting the focus of a megapixel network camera can be difficult due to the level of image detail. Therefore, the camera is also designed with VIVOTEK's Smart Focus System to make installation and adjustment easier by using remote focus and zoom adjustment.

The camera's IP67-rated housing is designed to protect the camera body from being immersed in the water, even against the immersion at the depth of at least 1m. Additionally, the wide temperature range further enhances the camera performance and reliability in extremely cold and hot weather.

Revision History

- Rev. 1.0: Initial release
- Rev. 1.1: Added non-heater models, IP8355H and IP8365H, in the technical specs.
- Rev. 1.2: Added a note about the DO pin output.
- Rev. 1.3: Corrected DO pin description.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

1. Package Contents

- IP8355, IP8355EH, IP8365, or IP8365EH
- Sun Shield / Wrench / RJ45 Female / Female Coupler / Double-sided Tape / Screws
- Wall mount bracket (w/ screws and anchors)
- Waterproof Connector for RJ45 Ethernet Enclosure
- Waterproof Connector (for backup use)
- Alignment Sticker / Desiccant Bag
- Software CD
- Quick Installation Guide

Symbols and Statements in this Document

INFORMATION: provides important messages or advices that might help prevent inconvenient or problem situations.

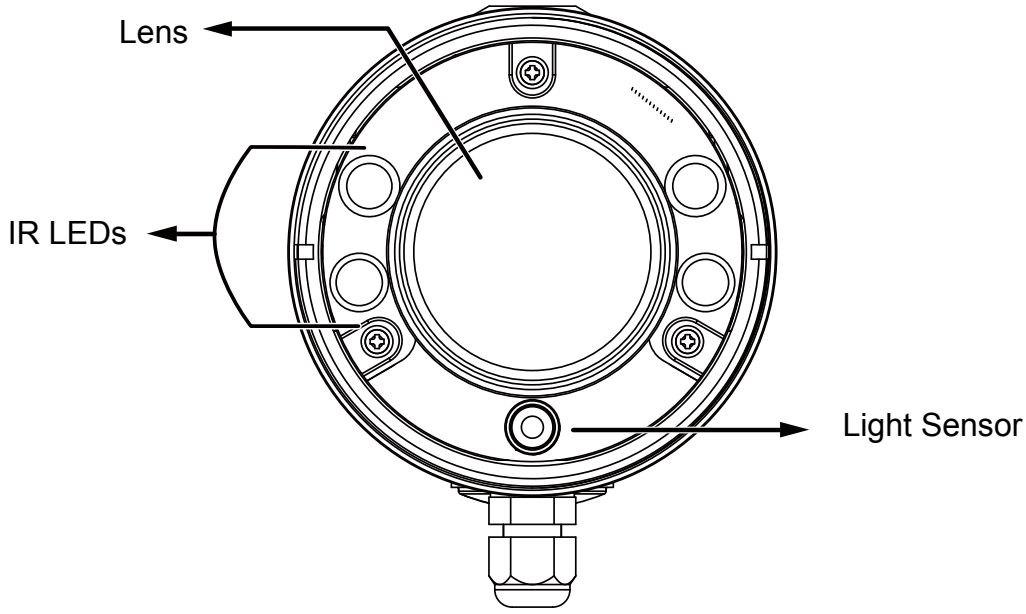
NOTE: Notices provide guidance or advices that are related to the functional integrity of the machine.

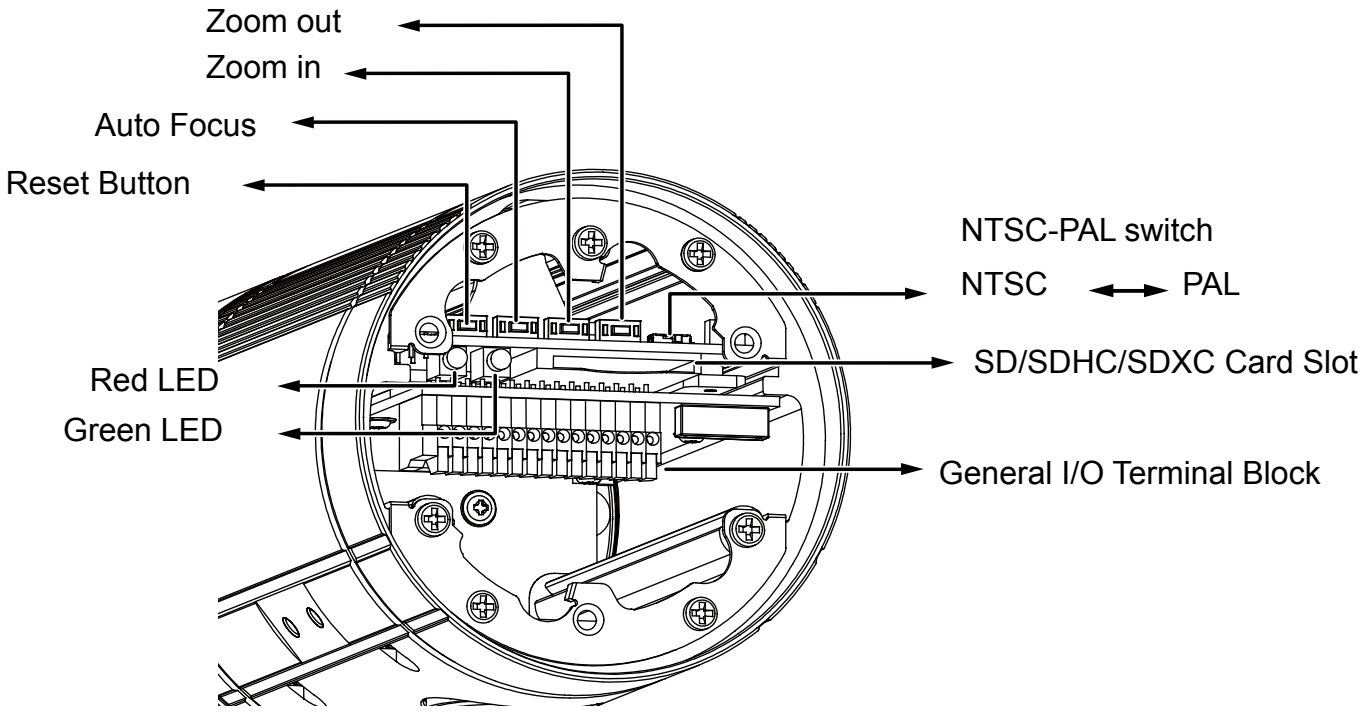
Tips: Tips are useful information that helps enhance or facilitae an installation, function, or process.

WARNING! or IMPORTANT!: These statements indicate situations that can be dangerous or hazardous to the machine or you.

Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

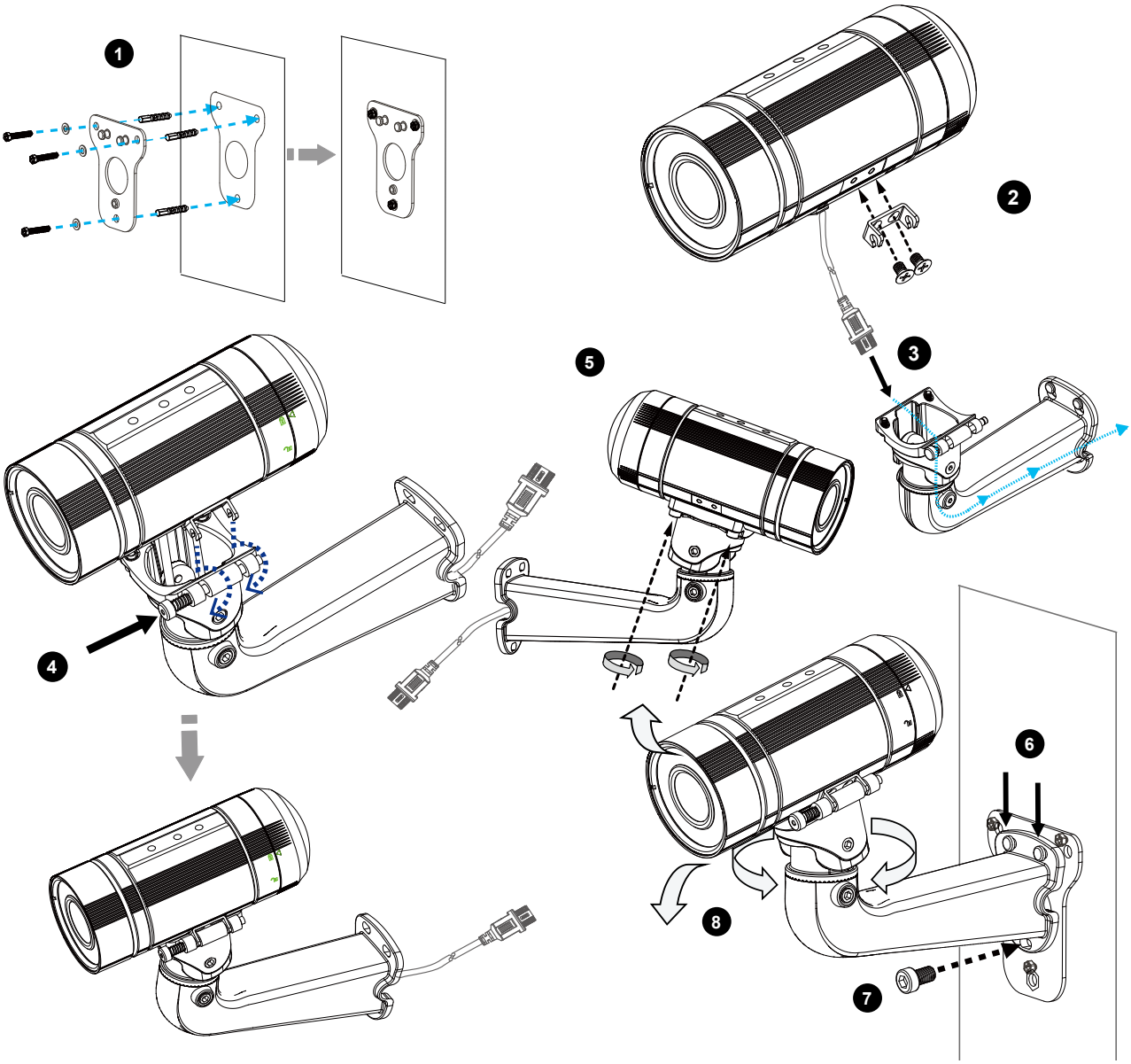
2. Physical Description





3. Hardware Installation

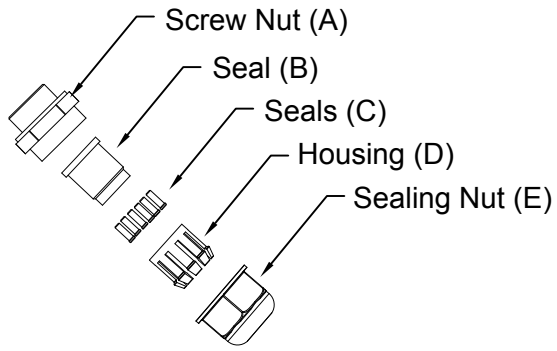
1. Attach the alignment sticker to the wall. Drill four holes into the wall. Then hammer the supplied plastic anchors into the holes and secure the plate with supplied screws.
2. Fix the intersection bracket to the side of the Network Camera with two screws.
3. Feed the RJ45 cable through the front opening of the wall mount bracket. (If you want to use external devices such as sensors and alarms, please refer to the assembling steps on the next page.)
4. Push the spring mortise and hook the bracket onto the groove of the wall mount bracket.
5. Secure the two screws on the other side of the wall mount bracket.
6. Hang the wall mount bracket to the mounting plate.
7. Fix the wall mount bracket with the supplied screw.
8. Adjust the angle of the wall mount bracket to aim at the shooting area.



4. Cabling Assembly

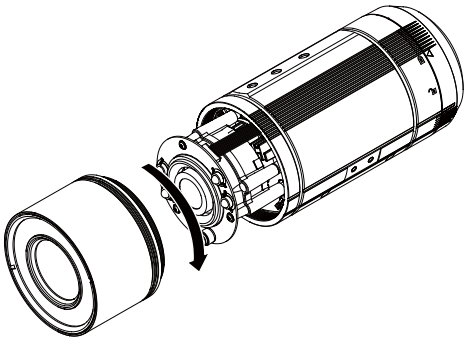
Waterproof Connector

Components of the Waterproof Connector

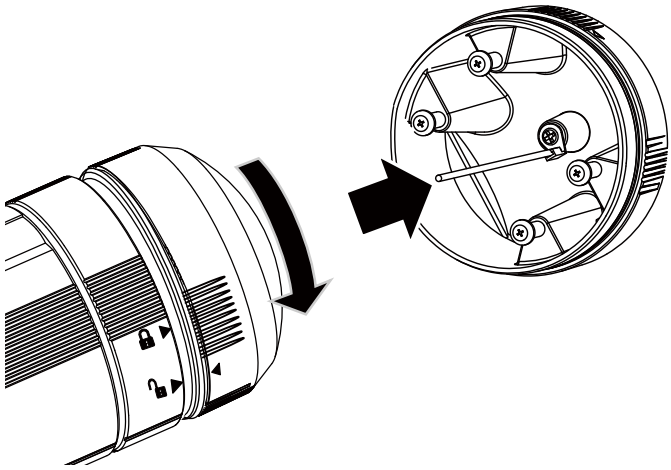


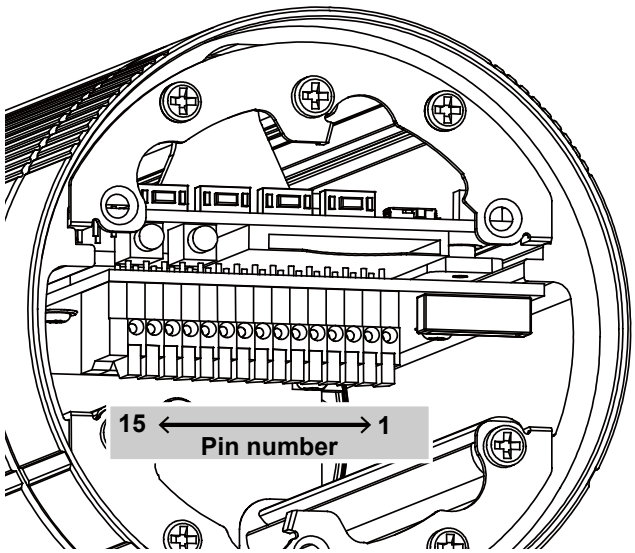
IMPORTANT:

If you should need to open the front cover, make sure you tighten it up later so that the camera can be waterproof.



Pin Definitions



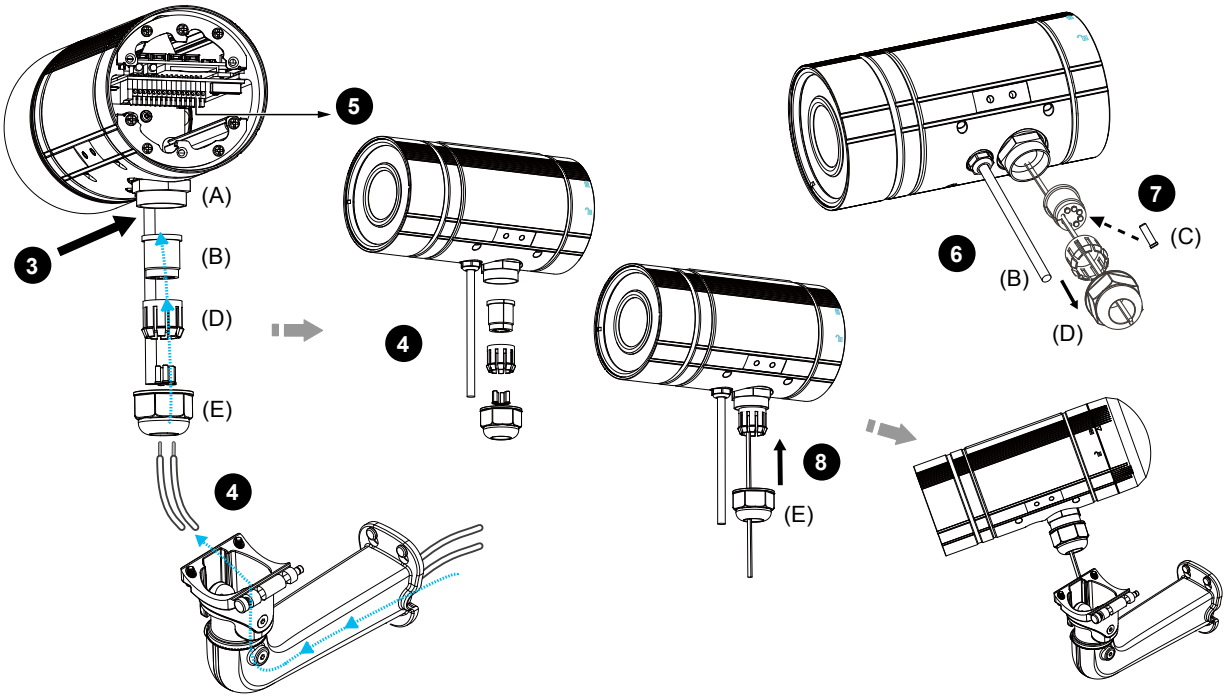


Pin Definitions

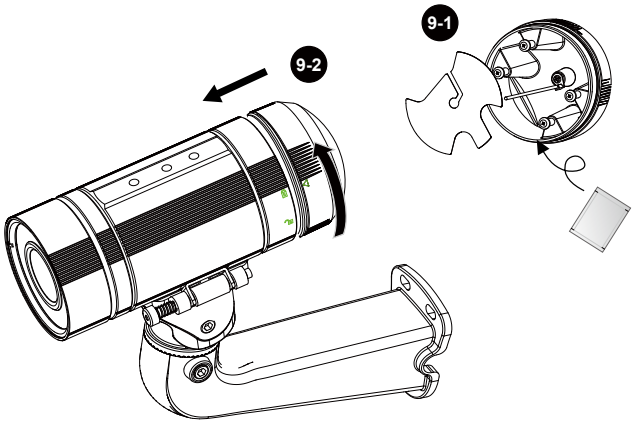
1	AC 24V IN
2	AC 24V IN
3	DC12V+ IN
4	DC12V- IN
5	DI-
6	DI+
7	DO-
8	DO+
9	N/C
10	N/C
11	EXT_MIC
12	Audio Out
13	Audio GND
14	TV Out
15	GND

Assembling Steps

1. Disassemble the components of the waterproof connector into part (A) ~ (E) as shown above.
2. Open the rear cover of the Network Camera.
3. Remove the rubber stopper from the bottom of the Network Camera and secure the screw nut (A) tightly.
4. You may choose to use AC24V or DC12V inputs as power source, please feed the power lines through the wall mount bracket and the waterproof connector (E --> D --> B --> A) as illustrated below. Pass power lines through the rubber seal (B) and then connect the power lines to the terminal block.
5. If you have external devices such as sensors and alarms, feed the cables through the wall mount bracket and the waterproof connector (E --> D --> B --> A) as the illustration shown below. Then refer to the pin definition to connect them to the general I/O terminal block. Note: The recommended cable gauge is 2.0 ~ 2.8 mm.
6. Push the seal (B) into the housing (D).
7. Insert the seals (C) into the empty holes on the seal (B) to avoid moisture.
8. Secure the sealing nut (E) tightly.

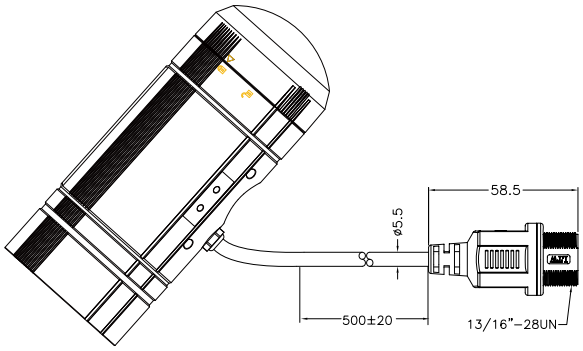


9. Open the aluminum foil vacuum bag and take out the desiccant bag. Attach the desiccant bag to the inner side of the rear cover, to under the insulation pad, and then tighten the rear cover. (Please replace the desiccant bag with a new one whenever you open the rear cover.)

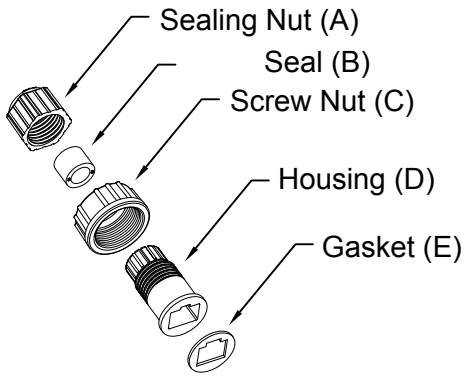


RJ45 Cable Connector

RJ45 Cable Dimension (unit: mm)

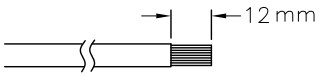


Components of the Waterproof Connector



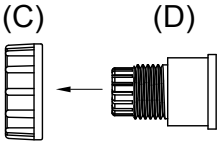
Assembling Steps

1. Prepare an Ethernet cable and strip part of the sheath.

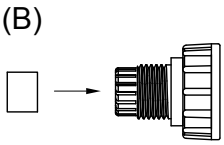


Recommended cable gauge: O.D. 5.5~7

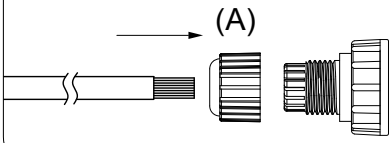
2. Insert the housing into the screw nut.



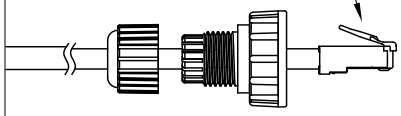
3. Insert the seal into the housing.



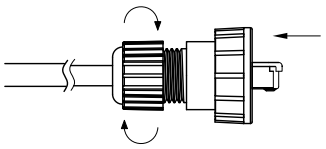
4. Insert the stripped Ethernet cable through the sealing nut and the housing.



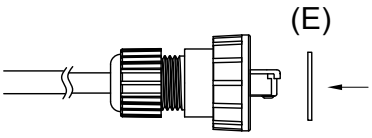
5. Clamp the cable with an RJ45 plug.



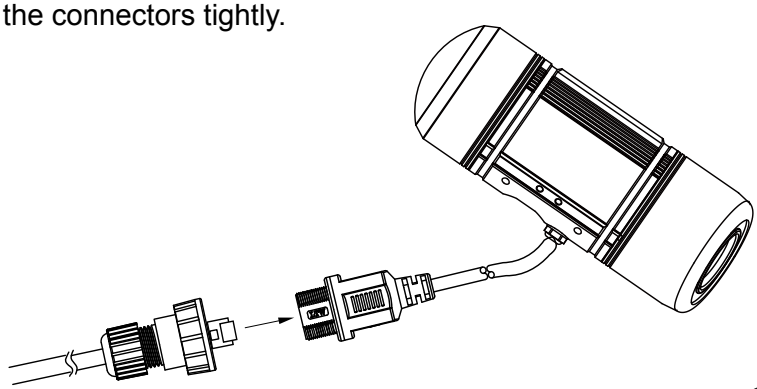
6. Push the RJ45 plug into the housing, then secure the sealing nut tightly.



7. Attach the gasket to the front of the housing.



8. Connect the Ethernet cable to the RJ45 cable and secure the connectors tightly.

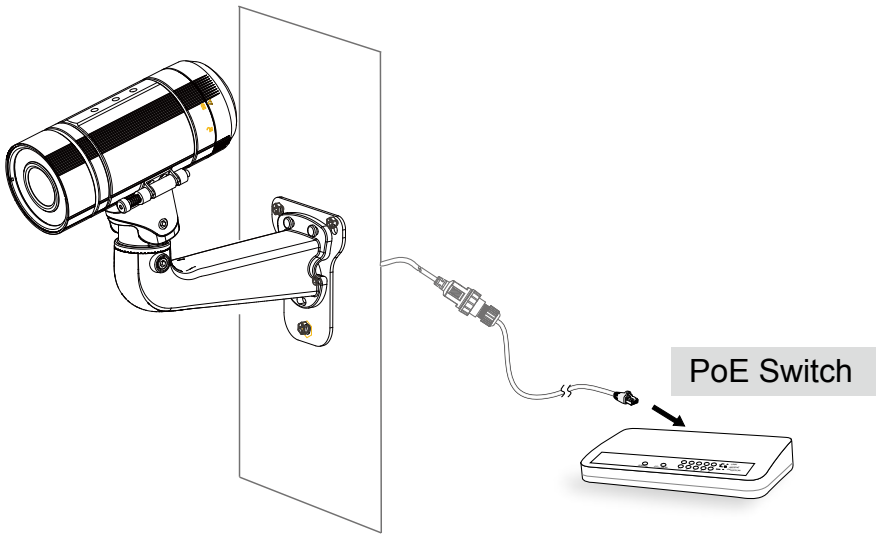


5. Network Deployment

Power over Ethernet (PoE)

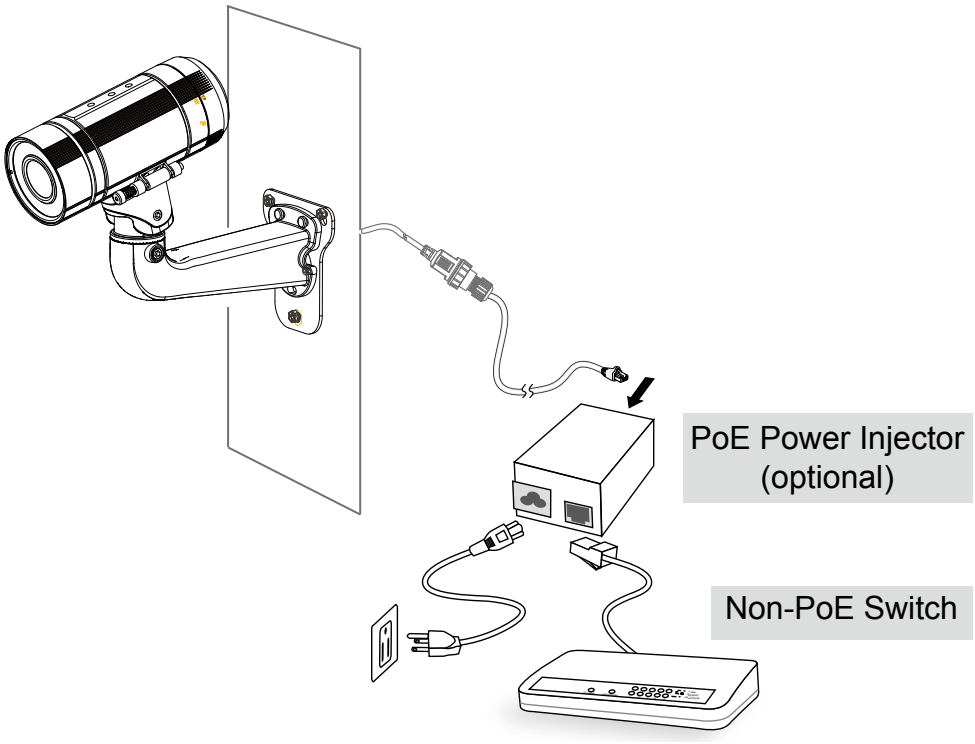
When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via Ethernet cable.



When using a non-PoE switch

Use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



Status LED

The LED indicates the status of the Network Camera.

Item	LED status	Description
1	Green and Red lit for once, and then turn steady red	Power on and system booting
	Red LED off	Power off
2	Steady Red and Green blinking every 1 sec.	Network normal (heartbeat)
	Steady Red and Green LED is off	Network failed
3	Red blinking every 0.15 sec., and Green LED blinking every 1 sec.	Upgrading firmware
4	Red blinking every 0.15 sec. and Green LED blinking every 0.15 sec.	Restoring default

General I/O Terminal Block

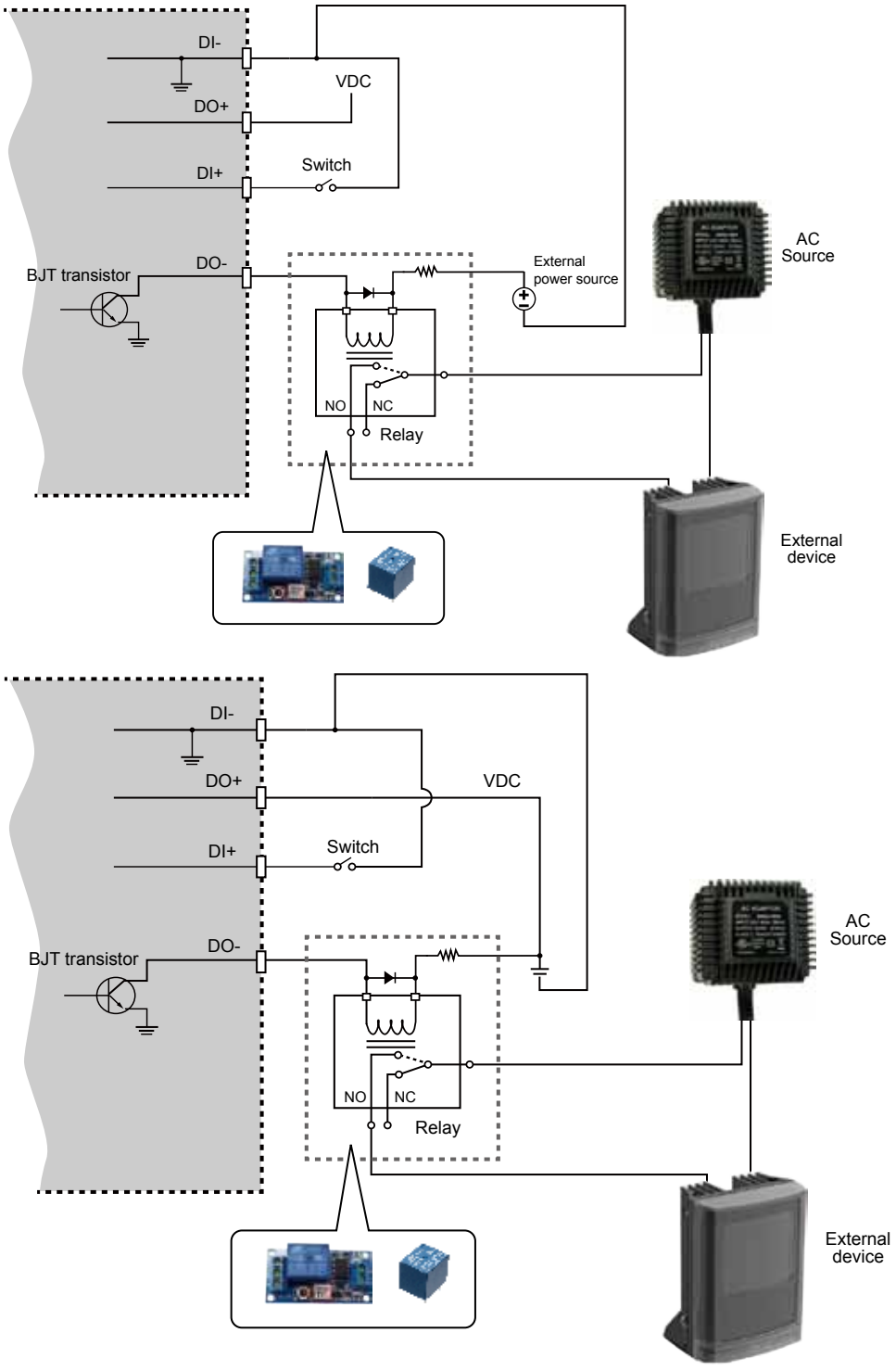
This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below. The 24V AC and DC 12V can be used as an alternate power source.

NOTE:

- The max. load for power output pin 8, 12V DO, is 50mA.
- If using the DC 12V power source, the DO output can be lowered to 11.2V.

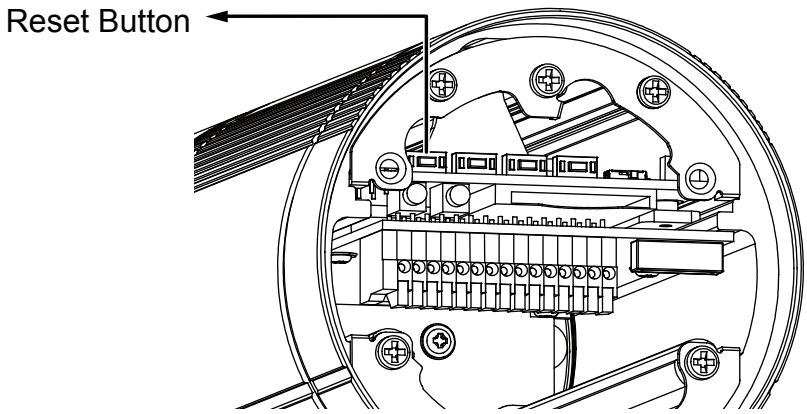
1	AC 24V IN
2	AC 24V IN
3	DC12V+ IN
4	DC12V- IN
5	DI-
6	DI+
7	DO-
8	DO+
9	N/C
10	N/C
11	EXT_MIC
12	Audio Out
13	Audio GND
14	TV Out
15	GND

DI/DO Diagram



1. The DO+ pin provides 12V output voltage, and the max. load is 50mA.
2. The max. voltage for DO- pins is 80VDC (External power).
   In order to control AC devices, the above diagram can be taken in consideration. The diagram uses a relay to control the ON/OFF condition of the AC device.
3. An external relay can be triggered by using DO+ or by an external power source, depending on the type of relay you use.
4. In case of using an individual relay (instead of using a relay module), for protection against voltage or current spikes, a transient voltage suppression diode must be connected in parallel with the inductive load.

Hardware Reset



The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

Restore: Press and hold the recessed reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

Micro SD/SDHC/SDXC Card Capacity

This network camera is compliant with **Micro SD/SDHC/SDXC 8GB, 16GB, or 64GB** and other preceding standard SD cards.

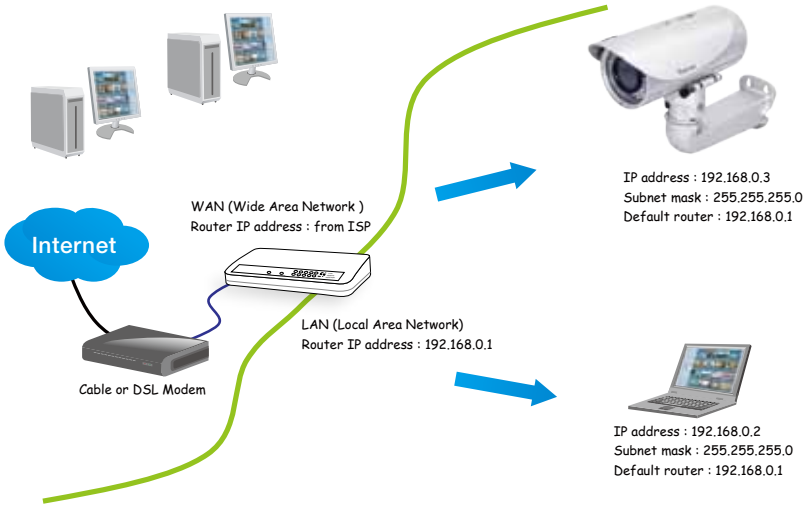
WARNING:

You will find a dessicant bag attached to the dome cover. Replace the dessicant bag included in the camera with the one shipped within the accessory bag.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 17 for details.


Internet
WAN (Wide Area Network)
Router IP address : from ISP
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

   - HTTP port: default is 80
   - RTSP port: default is 554
   - RTP port for audio: default is 5558
   - RTCP port for audio: default is 5559
   - RTP port for video: default is 5556
   - RTCP port for video: default is 5557

   If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 63 for details.

For example, your router and IP settings may look like this:

Device	IP Address: internal port	IP Address: External Port (Mapped port on the router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

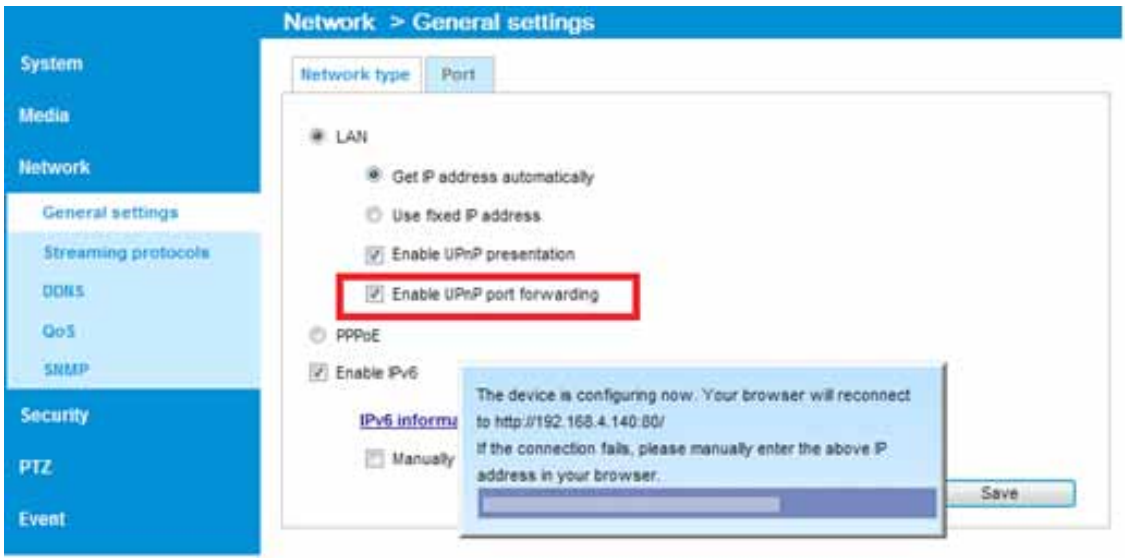
Configure the router, virtual server or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

When properly configured, you can access a camera behind the router using the HTTP request as follows: http://122.146.57.120:8000

If you change the port numbers on the Network configuration page, please open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. Please consult your network administrator for router configuration if you have troubles with the configuration.

For more information with network configuration options (such as that of streaming ports), please refer to Configuration > Network Settings. VIVOTEK also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.



Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN setting on page 63 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 64 for details.

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

1. Install IW2 under the Software Utility directory from the software CD. Double-click the IW2 shortcut on your desktop to launch the program.

2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.

3. The program will search for all VIVOTEK network devices on the same LAN.

4. After a brief search, the installer window will prompt. Click on the MAC and model name that matches the one printed on the product label. You can then double-click on the address to open a management session with the Network Camera.

Device Selection
Select a device to setup or upgrade
Installation Wizard 2
Smart Setup
Refresh Devices
MAC
IP Address
Model
00-02-D1-73-02-02
192.168.5.151
IP8365EH
0002D1730202
Please check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.
If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.
Network Camera
You can find the product label in the rear/bottom part of your device.

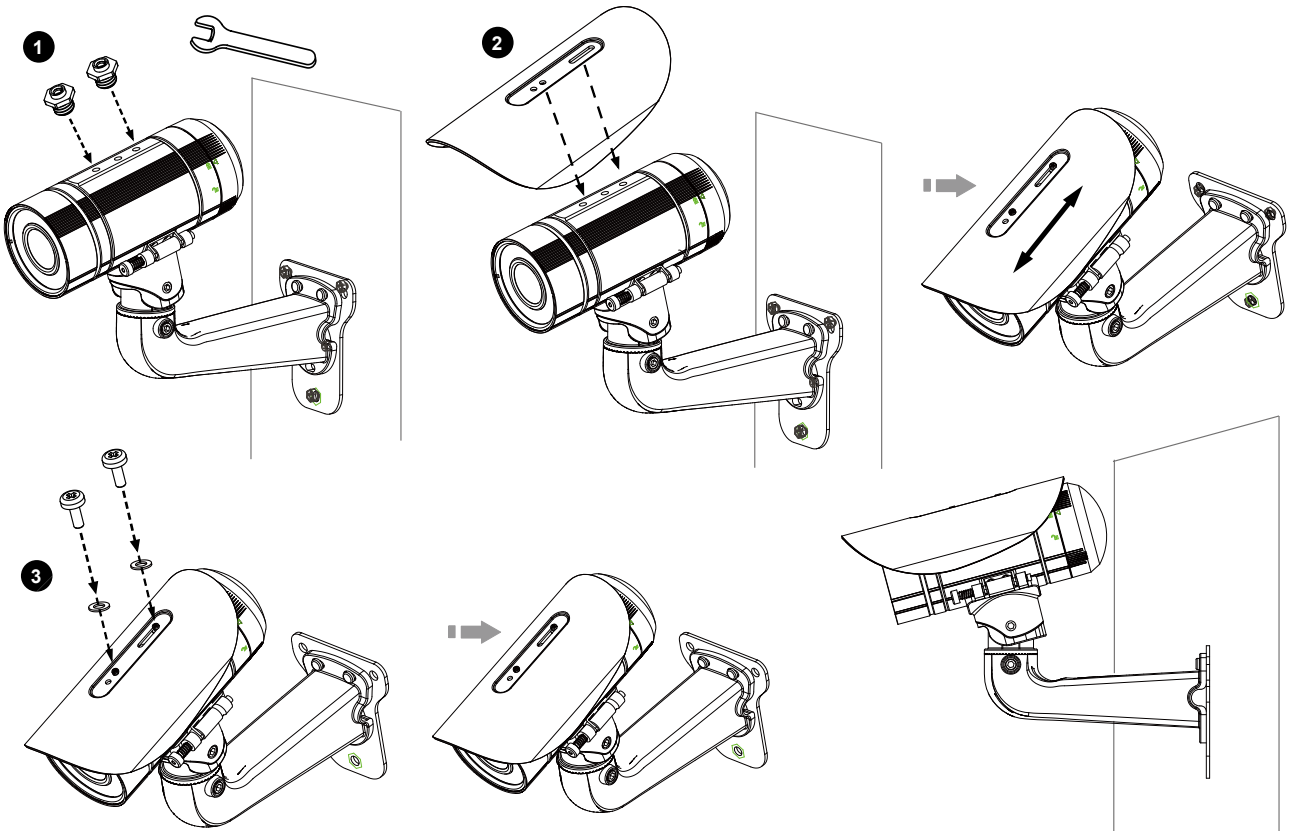
Ready to Use

1. A browser session with the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.

NOTE:

If you want to use the supplied sun shield for outdoor environments, please follow the steps below to install:

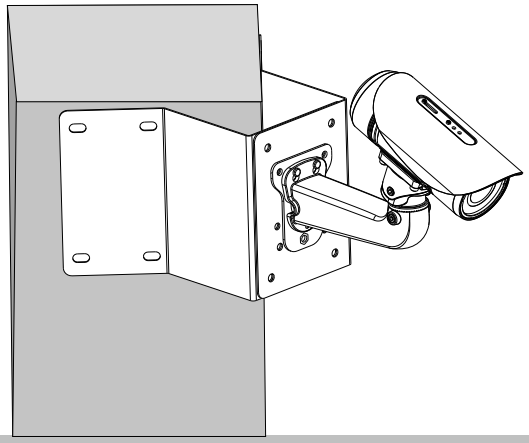
1. Tighten the supplied two hex couplers.
2. Attach the supplied sun shield to the Network Camera and slide it to the desired position.
3. Fix the sun shield with the supplied two screws.

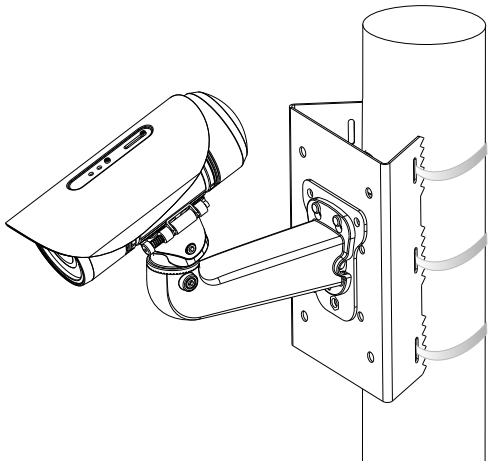


Accessories

VIVOTEK also provides other accessories for versatile applications as the following illustrations. Please visit VIVOTEK's official website for more purchase information.

Corner Mount Bracket	Pole Mount Bracket





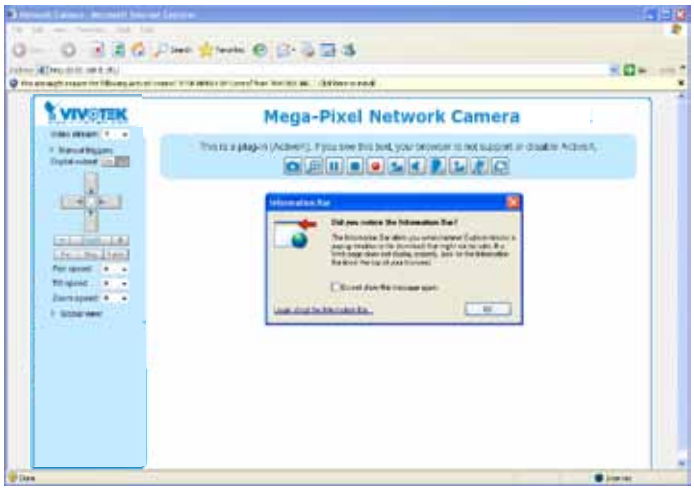
Accessing the Network Camera

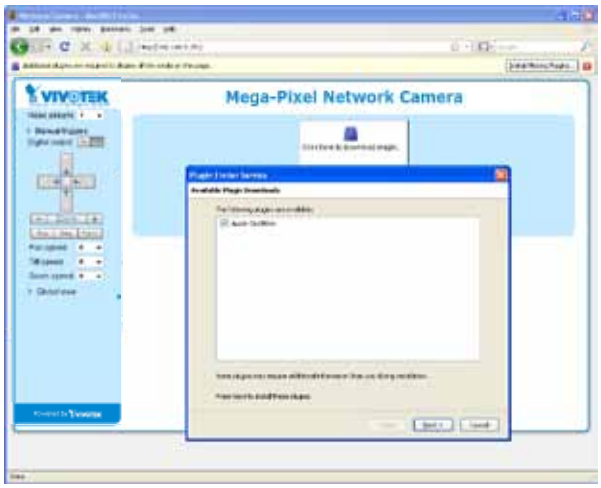
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access the Network Cameras on LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:

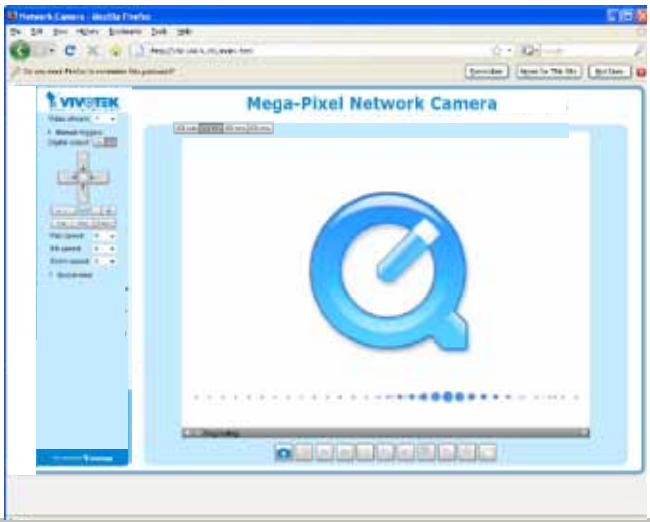
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Google Chrome).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.





NOTE:

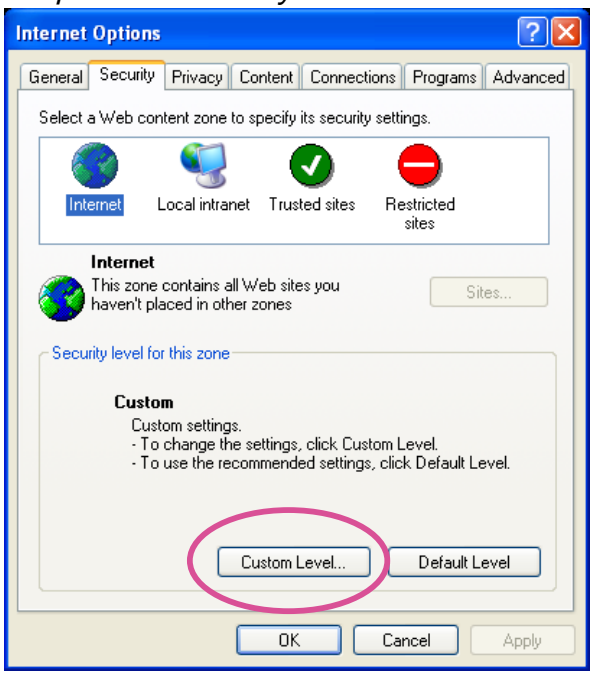
► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.*



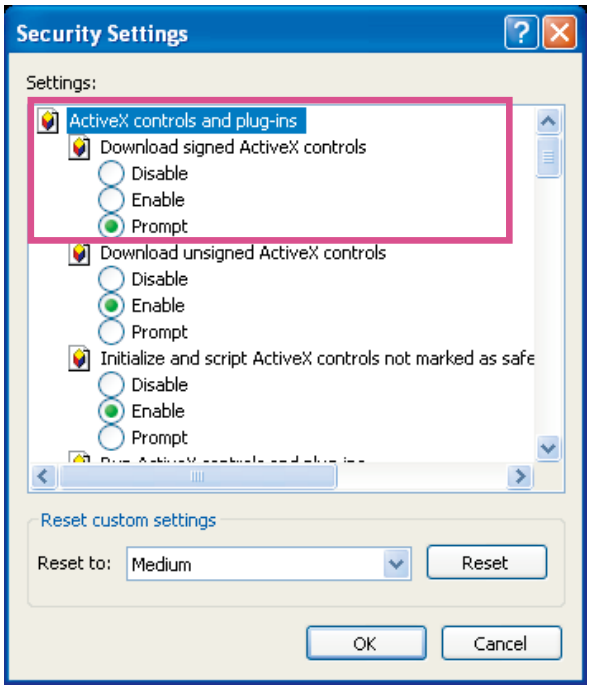
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 81.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



*2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



3. Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.

IMPORTANT:

1. Currently the Network Camera utilizes 32-bit ActiveX plugin. You CAN NOT open a management/view session with the camera using a 64-bit IE browser.
2. If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\SysWOW64. A 32-bit version of IE browser will be installed.
3. On Windows 7, the 32-bit explorer browser can be accessed from here:
   C:\Program Files (x86)\Internet Explorer\iexplore.exe

NOTE:

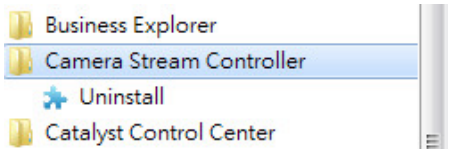
1. For a megapixel camera, it is recommended to use monitors of the 24" size or larger, and are capable of 1600x1200 or better resolutions.
2. Below are the defaults for Audio settings:
   For cameras with built-in microphone: **Not Muted.**
   For cameras without built-in microphone: **Muted.**

   To receive audio input from external microphone, you may need to enable the audio input from **Media** > **Audio**. Refer to page 62 for more information.

Tips:

- The onscreen Java control can malfunction under the following situations:

  A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.
- In the event of plug-in compatibility issues, you may try to uninstall the plug-in that was previously installed.



Using RTSP Players

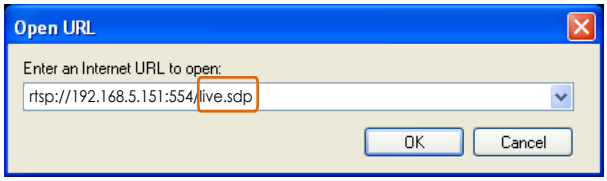
To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

VLC Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream #1, #2, #3, or #4>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 72.
For example:



4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 72 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 15.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 72.

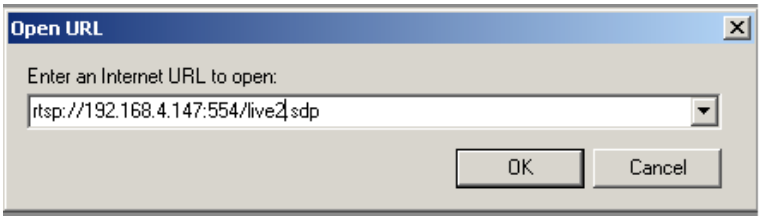
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Stream settings on page 58.

Video Mode	H.264
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (G.711)	PCMU

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 72.

4. Launch the player on the 3GPP-compatible mobile devices (e.g., VLC Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream # with small frame size and frame rate>.
   For example:



Using VIVOTEK Recording Software

The product software CD also contains an ST-7501 recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.

VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 36.

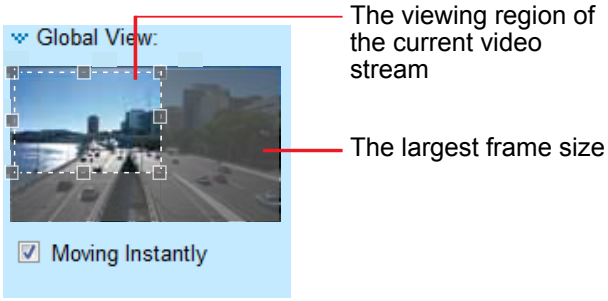
Camera Control Area

Video Stream: This Network Camera supports multiple streams (stream #1 and #2) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 58 for detailed information.

Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 3 event settings can be configured. For more information about event setting, please refer to page 97. If you want to hide this item on the homepage, please go to **Configuration> System > Homepage Layout > General settings > Customized button** to deselect “show manual trigger button”.

Digital Output: Click to turn the digital output device on or off.

Global View: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/ Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 94. For more information about how to set up the viewing region of the current video stream, please refer to page 60.



PTZ Panel: This Network Camera supports both “digital“ (e-PTZ) and “mechanical“ pan/tilt/zoom control. Please refer to PTZ settiings on page 94 for detailed information.

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 31.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 35.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. Please note that you can also change a language on the Configuration page; please refer to page 35.

Hide Button

You can click the hide button to hide the control panel or display the control panel.

Resize Buttons

:

Click the Auto button, the video cell will resize automatically to fit the monitor.
Click 100% is to display the original homepage size.
Click 50% is to resize the homepage to 50% of its original size.
Click 25% is to resize the homepage to 25% of its original size.

Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video Settings on page 48.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 31.

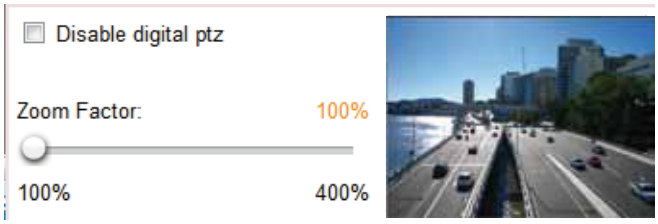
Time: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 48.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 48.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 32 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Media > Image on page 48.

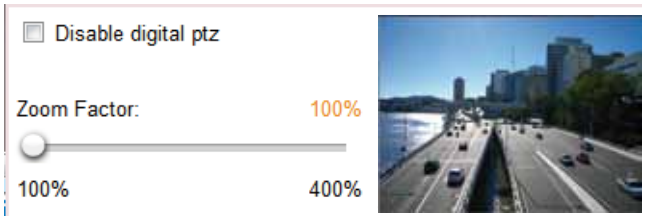
Time: Display the current time. For more information, please refer to Media > Image on page 48.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 48.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 32 for details.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

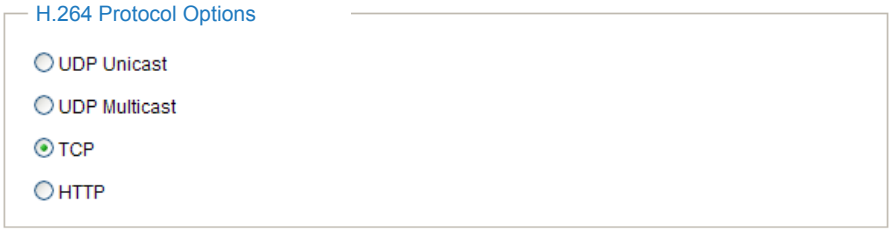
Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264 Protocol Options



Depending on your network environment, there are four transmission modes of H.264 or MPEG-4 streaming:

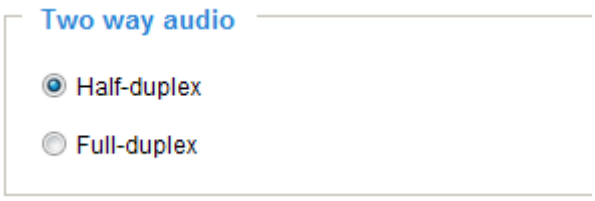
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 72.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

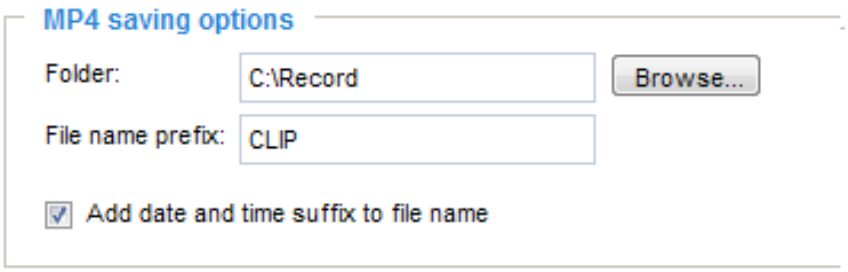
HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

Two way audio



Half duplex: Audio is transmitted from one direction at a time, e.g., from a PC holding a web console with the camera.
Full duplex: Audio is transmitted in both directions simultaneously.

MP4 Saving Options

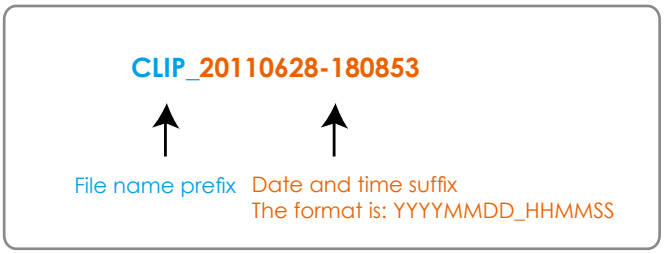


Users can record live video as they are watching it by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

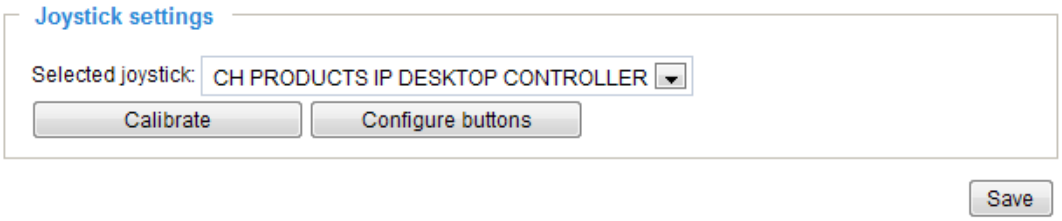
Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.



Local Streaming Buffer Time

In a busy network, fluctuations in available bandwidth can occur. Video streaming may lag and may not proceed very smoothly. If you enable this option, video streams from the camera will be temporarily stored on the computer's cache memory for a configurable period of time (seconds or milliseconds) before being played on a web session. This will help you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay for 3 seconds.

Joystick Settings



Enable Joystick

Connect to the USB plug of the joystick to a USB port on your management computer. Supported by the plug-in in the main page (Microsoft's DirectX), once the plug-in in the main page is loaded, it will automatically detect if there is any joystick on the computer. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices. Please follow the instructions below to enable joystick settings.

1. Right-click on a live view window. Select Joystick Settings. If your joystick is working properly, it will be displayed on the drop-down list.
2. Select the joystick you want to configure. Check **Enable Joystick**, then click **Configure Buttons** to open Buttons configuration window.

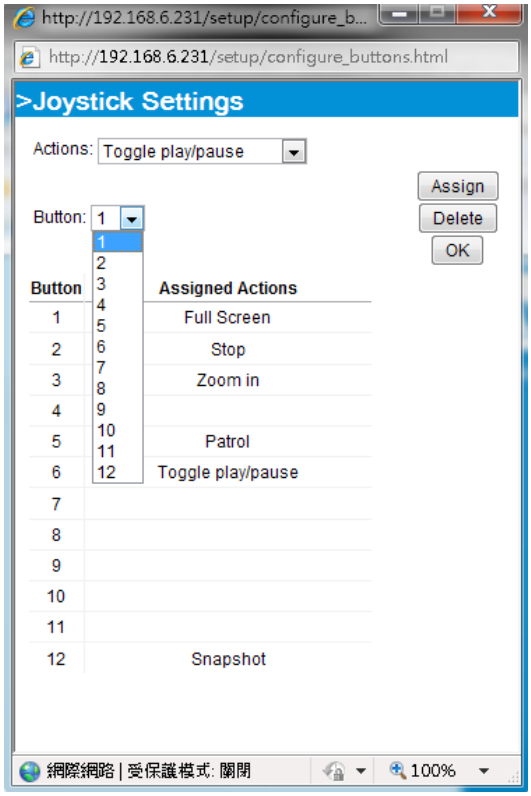
NOTE:

- If you want to assign Preset actions to your joystick, the preset locations should be configured in advance in the Configuration > PTZ page.
- If your joystick is not working properly, it may need to be calibrated. Click the **Calibrate** button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.
- The joystick will appear in the **Game Controllers** list in the Windows Control panel. If you want to check out for your devices, go to the following page: Start -> Control Panel -> Game Controllers.

Buttons Configuration

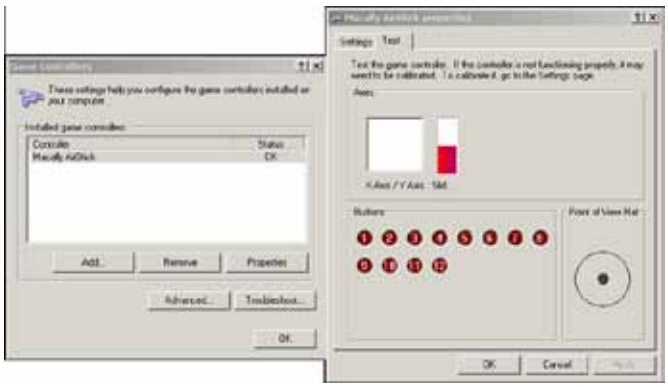
Click the **Configure Buttons** button, a window will prompt as shown below. Please follow the steps below to configure your joystick buttons:

1. Select a button number from the Button # pull-down menu.



Tips

If you are not sure of the locations of each button, use the **Properties** window in the **Game Controllers** utility.



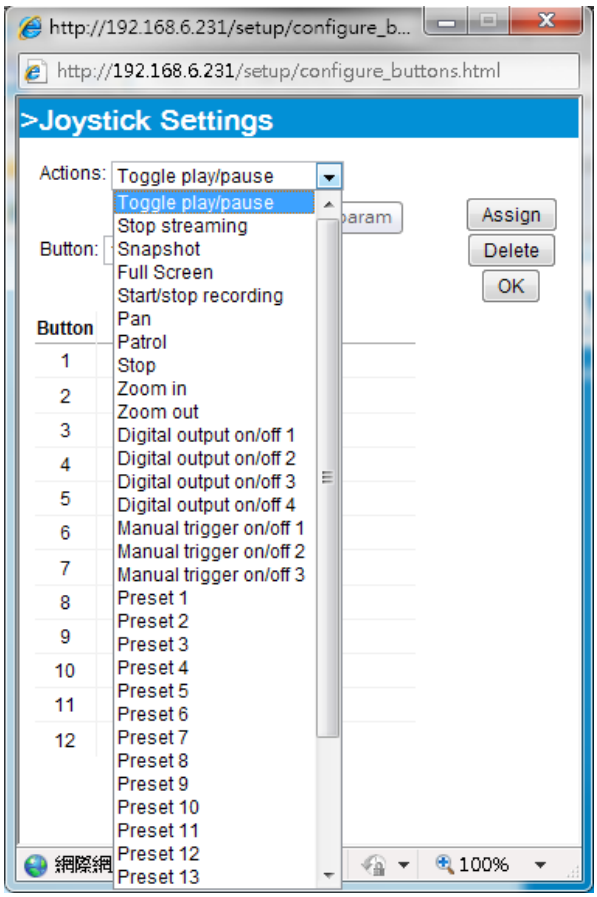
2. Select a corresponding action, such as Patrol or Preset#.

3. Click the **Assign** button to assign an action to the button. You can delete an association by selecting a button number, and then click the **Delete** button.

   Repeat the process until you are done with the configuration of all preferred actions.

   The buttons you define should appear on the button list accordingly.

4. Please remember to click the **Save** button on the Client settings page to preserver your settings.



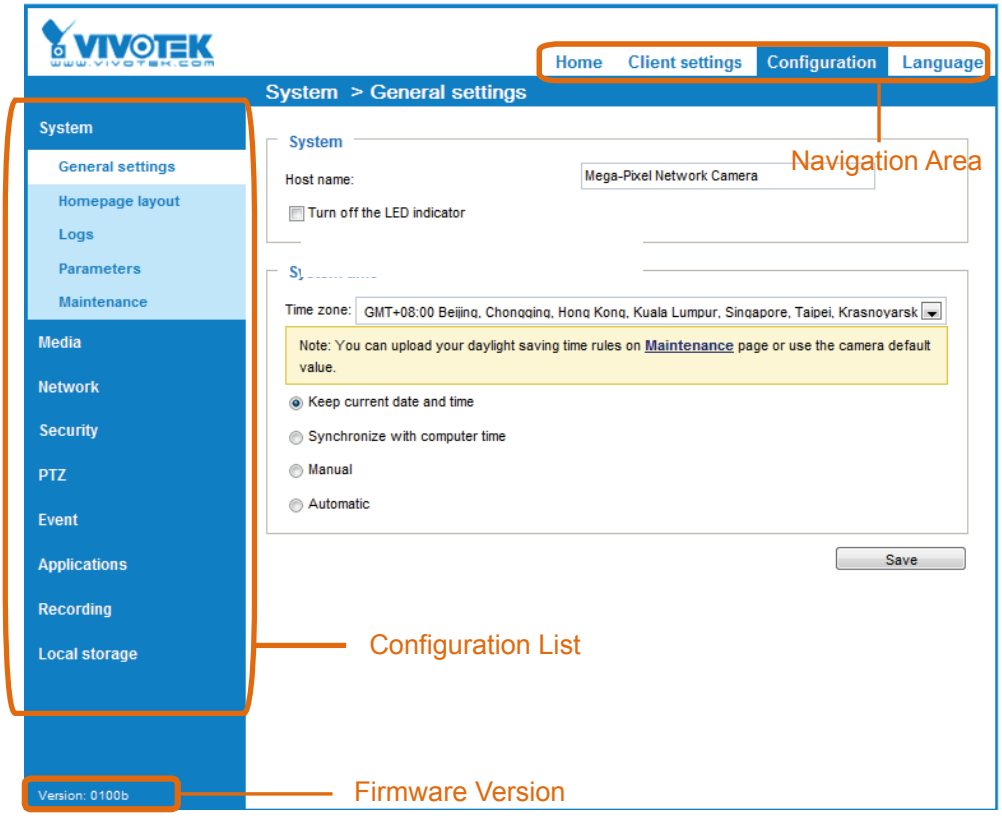
Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort.

In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the main page interface:



Each function on the configuration list will be explained in the following sections.
Navigation Area provides an instant switch among **Home** page (the monitoring page for live viewing), **Client settings**, **Configuration** page, and multi-language selection.

System > General settings

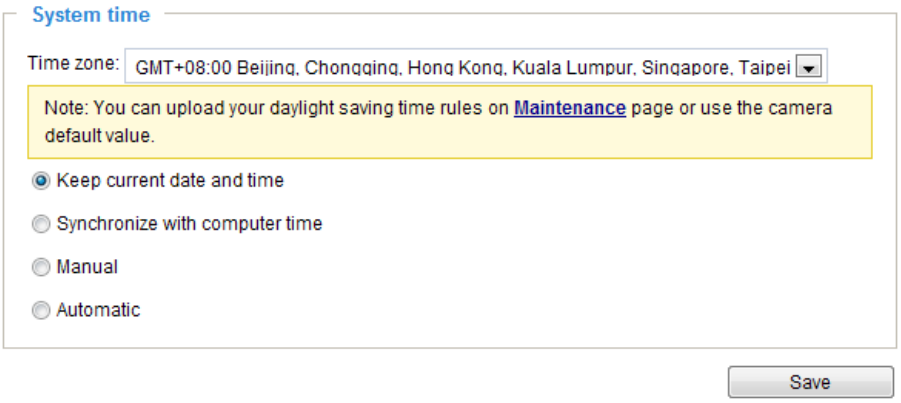
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System, and System Time. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page, and also on the view cell of ST-7501 and VAST management software.

Turn off the LED indicators: If you do not want others to notice the network camera is in operation, you can select this option to turn off the LED indicators.

System time


System time
Time zone:
GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei
Note: You can upload your daylight saving time rules on Maintenance page or use the camera default value.
Keep current date and time
Synchronize with computer time
Manual
Automatic
Save

Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Synchronize with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 45 for details.

System > Homepage layout

This section explains how to set up your own customized homepage layout.

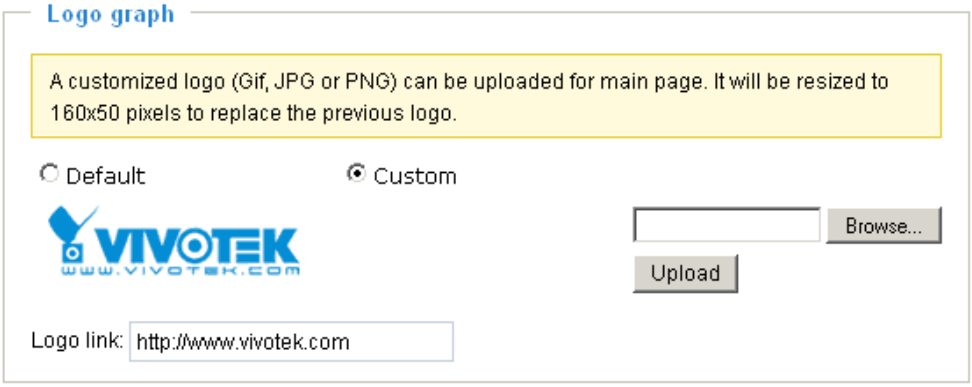
General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo graph

Here you can change the logo at the top of your homepage.



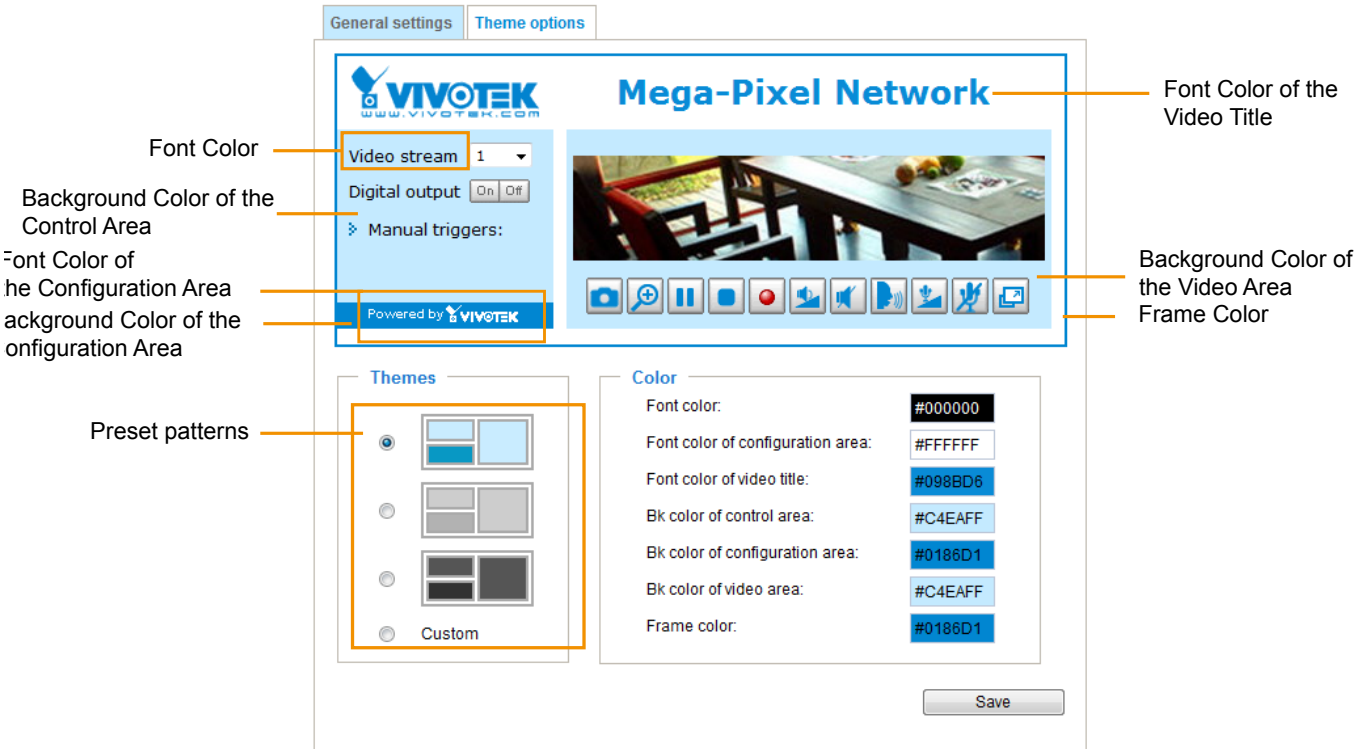
Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Customized button

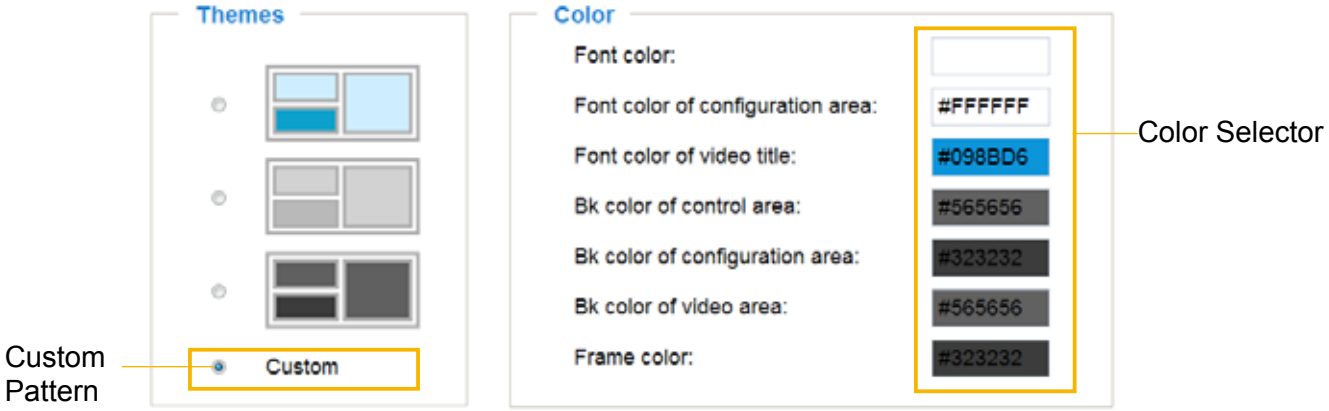
If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

Theme Options

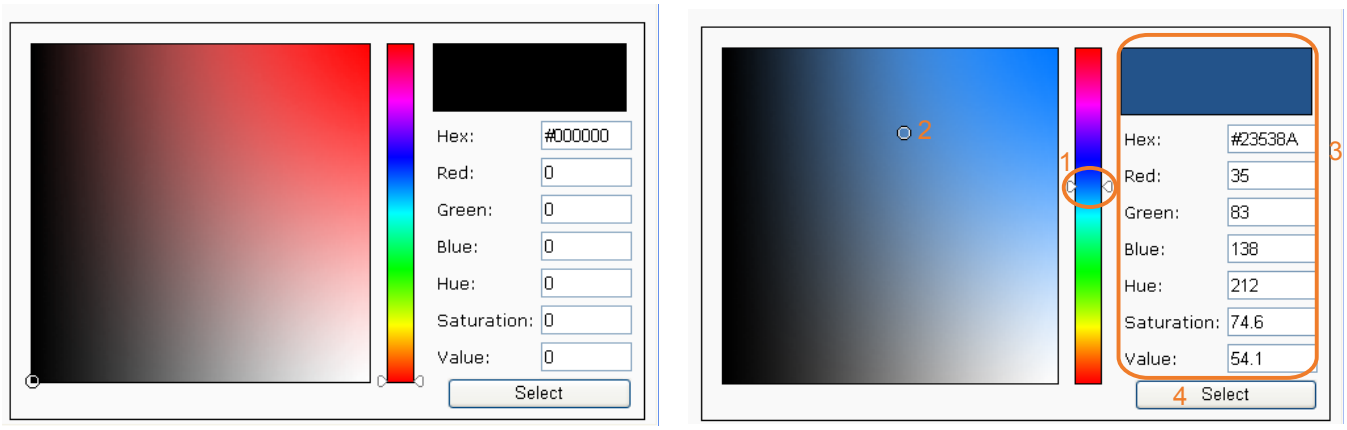
Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.



4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

System > Logs

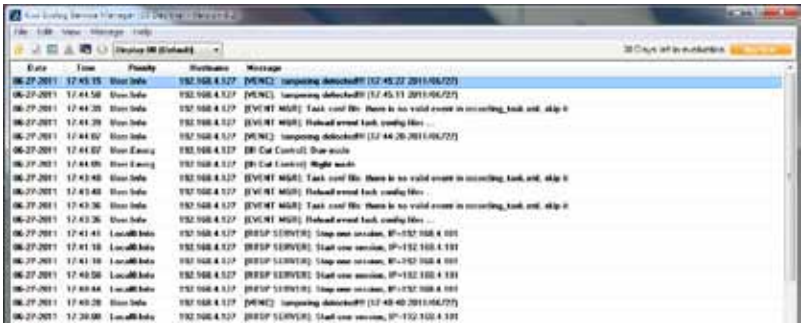
This section explains how to configure the Network Camera to send the system log to a remote server as backup.

Log server settings

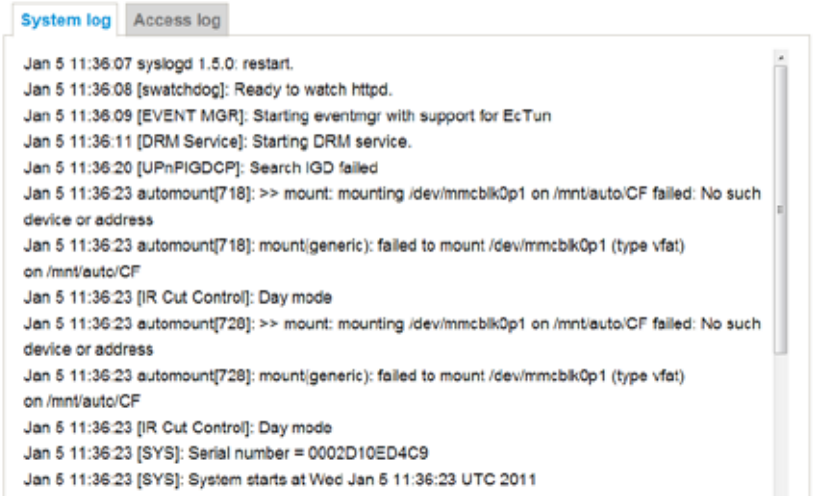
Follow the steps below to set up the remote log:

1. Select **Enable remote log**.
2. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

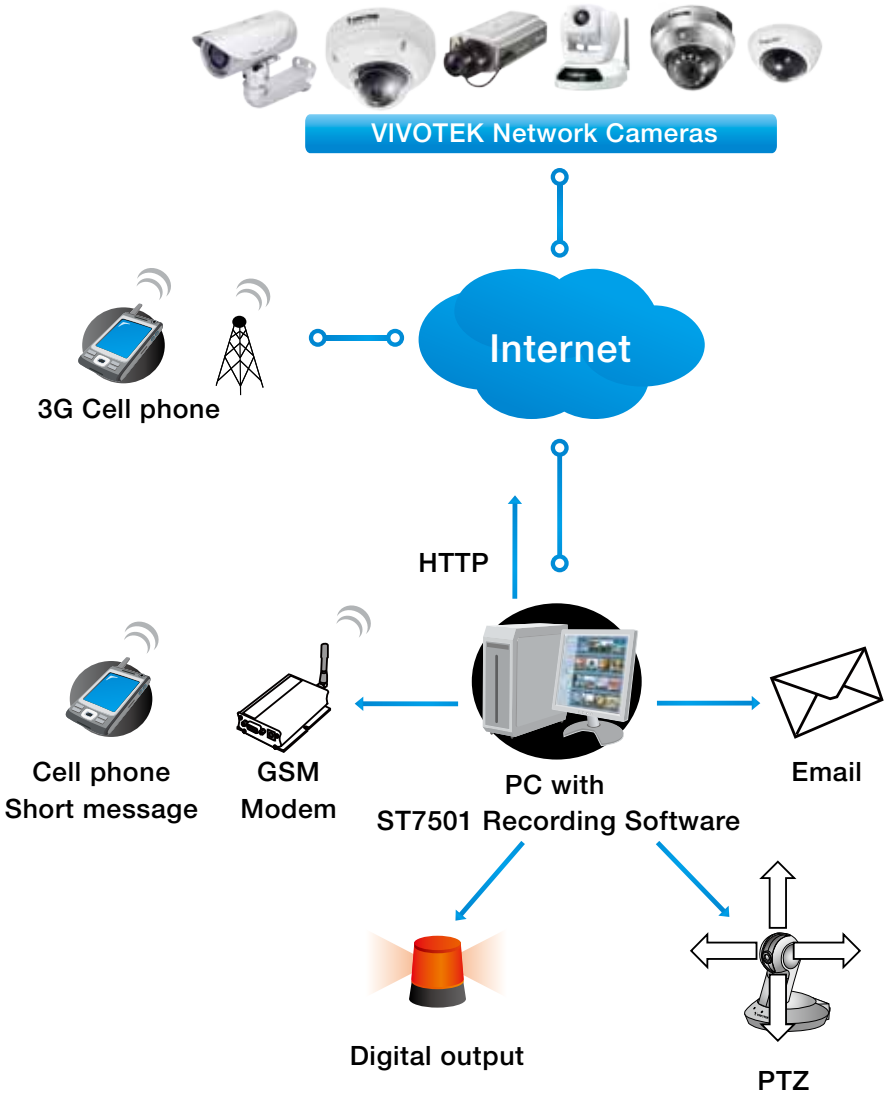


System log

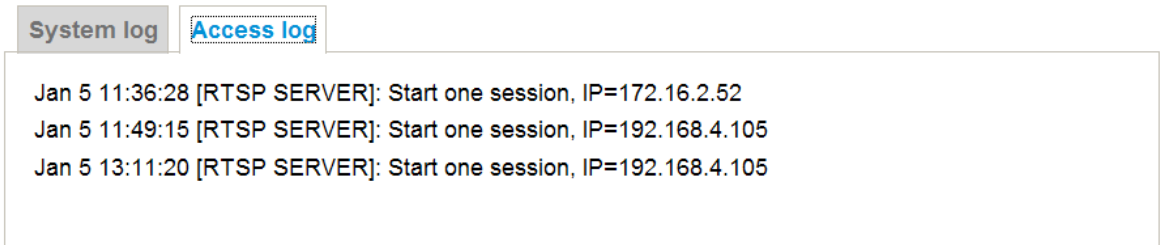

System log
Access log
Jan 5 11:36:07 syslogd 1.5.0: restart.
Jan 5 11:36:08 [swatchdog]: Ready to watch httpd.
Jan 5 11:36:09 [EVENT MGR]: Starting eventmgr with support for EcTun
Jan 5 11:36:11 [DRM Service]: Starting DRM service.
Jan 5 11:36:20 [UPnPIGDCP]: Search IGD failed
Jan 5 11:36:23 automount[718]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address
Jan 5 11:36:23 automount[718]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Jan 5 11:36:23 [IR Cut Control]: Day mode
Jan 5 11:36:23 automount[728]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address
Jan 5 11:36:23 automount[728]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Jan 5 11:36:23 [IR Cut Control]: Day mode
Jan 5 11:36:23 [SYS]: Serial number = 0002D10ED4C9
Jan 5 11:36:23 [SYS]: System starts at Wed Jan 5 11:36:23 UTC 2011

This column displays the system log in a chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

You can install the included ST7501 recording software, which provides an Event Management function group for delivering event messages via emails, GSM short messages, onscreen event panel, or to trigger an alarm, etc. For more information, refer to the ST7501 User Manual.



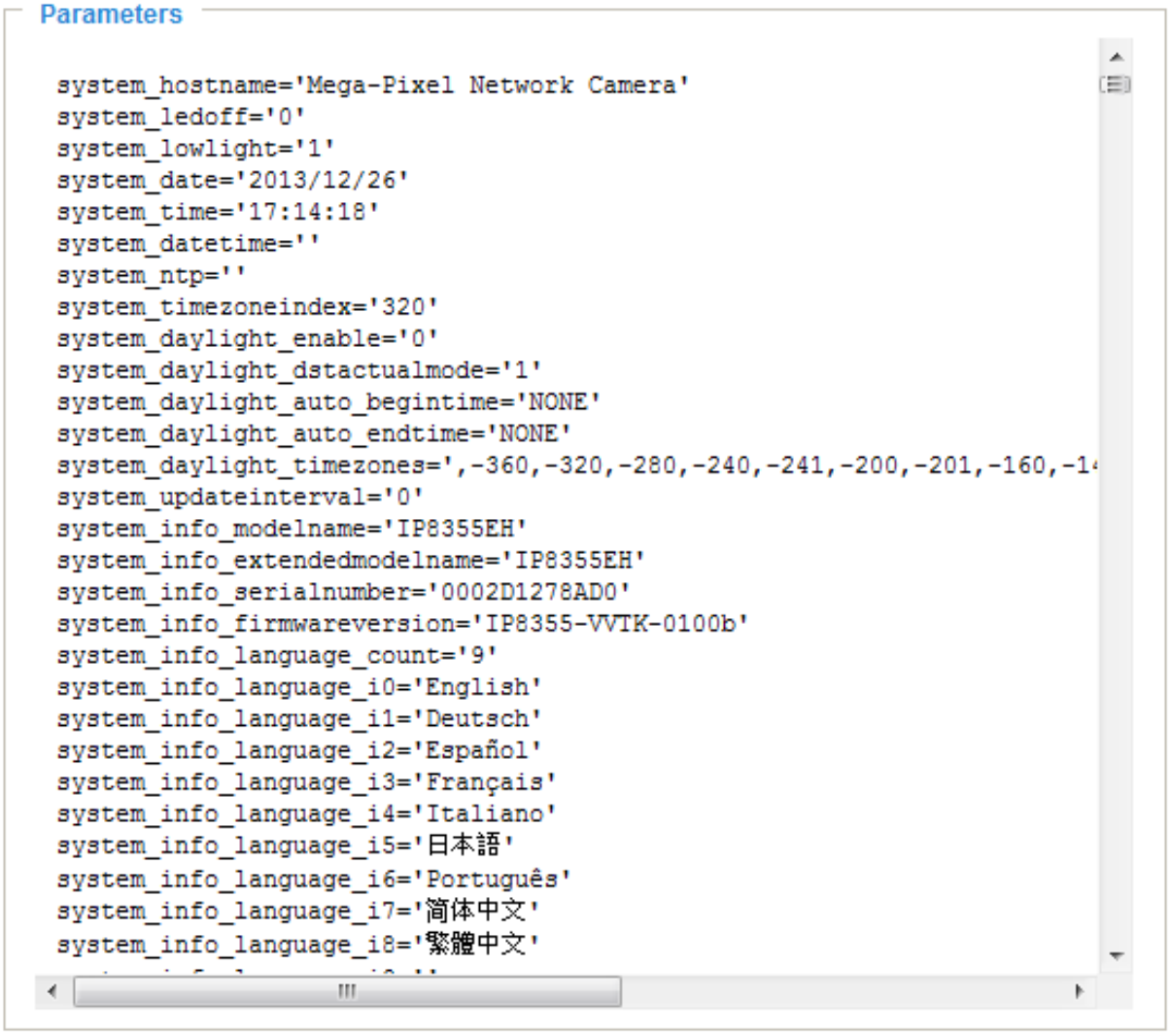
Access log


System log
Access log
Jan 5 11:36:28 [RTSP SERVER]: Start one session, IP=172.16.2.52
Jan 5 11:49:15 [RTSP SERVER]: Start one session, IP=192.168.4.105
Jan 5 13:11:20 [RTSP SERVER]: Start one session, IP=192.168.4.105

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

System > Parameters

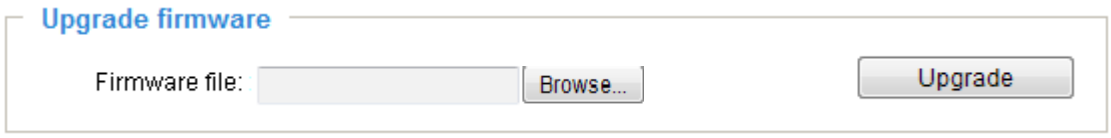
The View Parameters page lists the entire system's parameters. If you need technical assistance, please provide the information listed on this page.



System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

General settings > Upgrade firmware

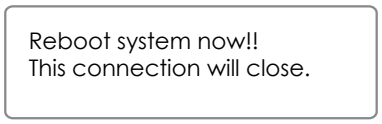


This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

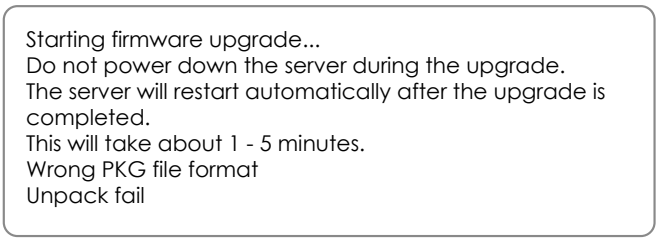
Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.

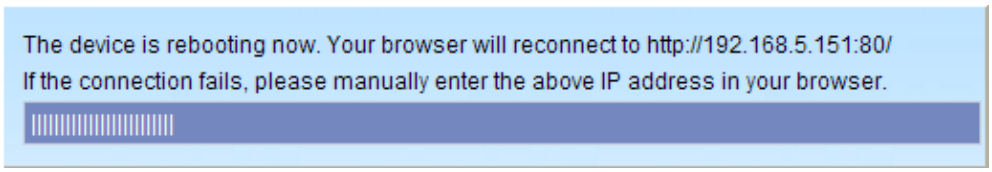


The following message is displayed when you have selected an incorrect firmware file.


Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

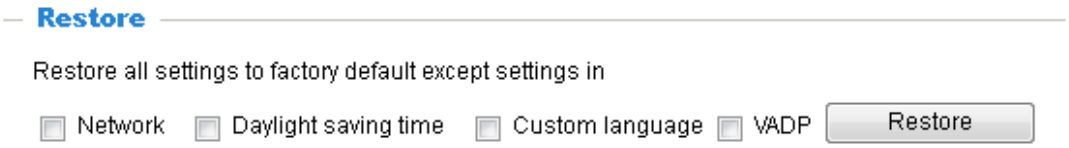
General settings > Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

General settings > Restore



This feature allows you to restore the Network Camera to factory default settings.

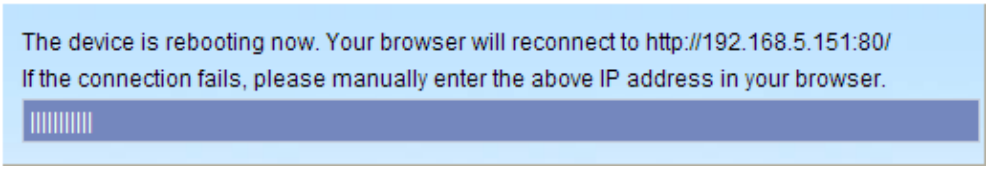
Network: Select this option to retain the Network Type settings (please refer to Network Type on page 63).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

Custom Language: Select this option to retain the Custom Language settings.

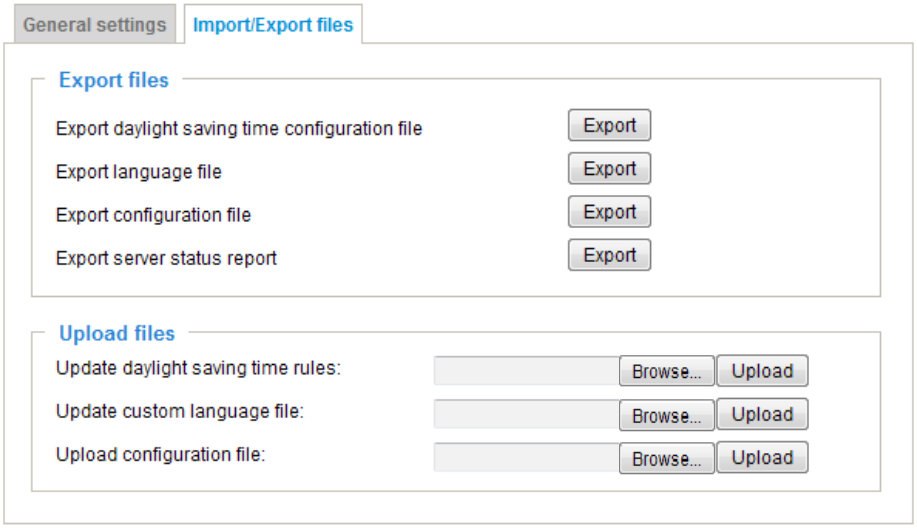
VADP: Retain the VADP modules (3rd-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

Import/Export files

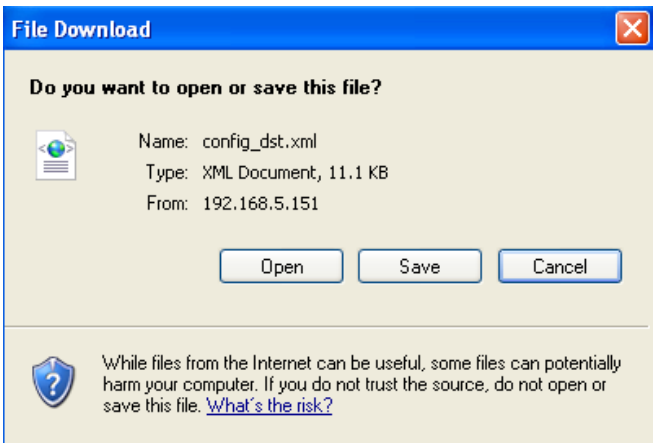
This feature allows you to Export / Update daylight saving time rules, custom language file, configuration file, and server status report.



Export daylight saving time configuration file: Click to set the start and end time of DST (Daylight Saving).

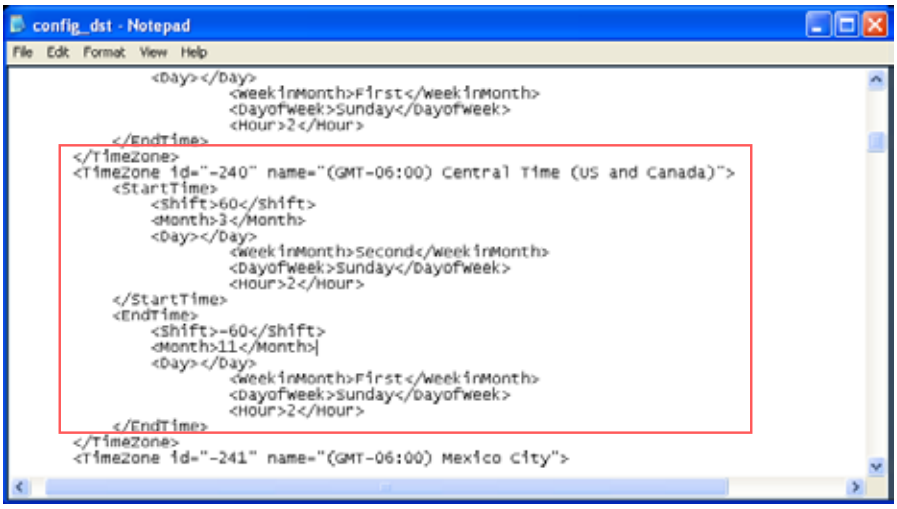
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.


File Download
Do you want to open or save this file?
Name: config_dst.xml
Type: XML Document, 11.1 KB
From: 192.168.5.151
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

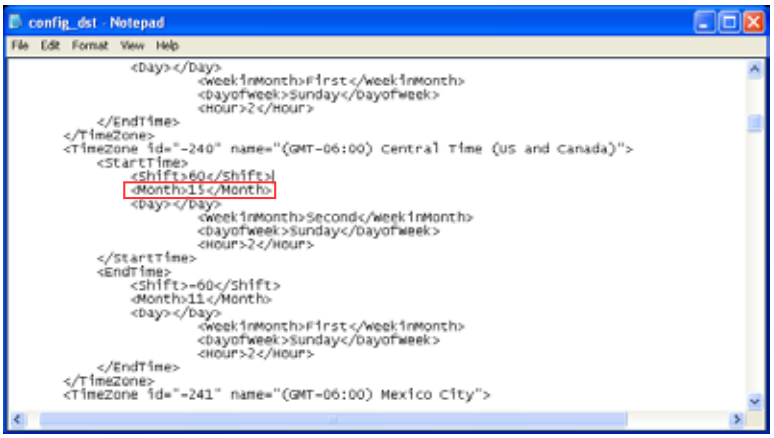
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

   In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.

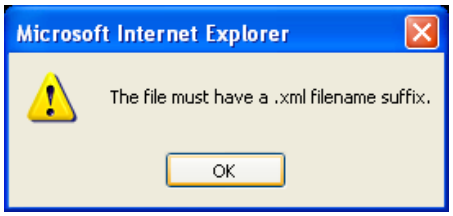


Update daylight saving time rules: Click **Browse…** and specify the XML file to update.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



The following message is displayed when attempting to upload an incorrect file format.



Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Update custom language file: Click **Browse…** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server staus report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message ... and so on.

Tips:

- If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

  Applicable scenario:

  (1) Power disconnected during firmware upgrade.
  (2) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

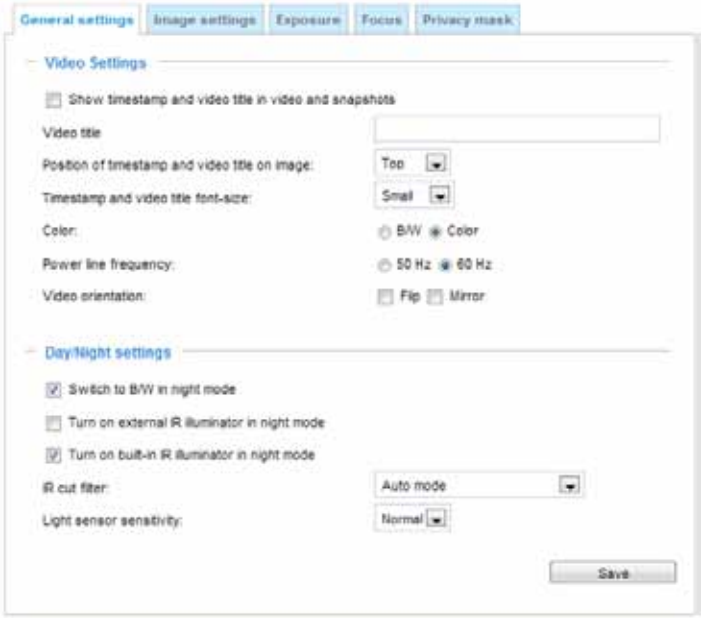
  You can use the following methods to activate the camera with its backup firmware:

  (1) Press and hold down the reset button for at least one minute.
  (2) Power on the camera until the Red LED blinks rapidly.
  (3) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When tthis process is completed, the LED status should return to normal.

Media > Image

This section explains how to configure the image settings of the Network Camera. It is composed of the following five columns: General settings, Image settings, Exposure, Focus, and Privacy mask.

General settings



Video title

Show_timestamp_and video_title_in_video_and_snapshots: Enter a name that will be displayed on the title bar of the live video as shown below.

Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

Timestamp and video title font size: Select the font size for the time stamp and title.

Color: Select to display color or black/white video streams.

Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

Timestamp and video title font size: Select the font size for the time stamp and title.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Video orientation: Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that if you have preset locations, those locations will be cleared after flip/mirror setting.

Day/Night Settings

Switch to B/W in night mode
Select this to enable the Network Camera to automatically switch to Black/White during night mode.

Turn on external IR illuminator in night mode
Select this to turn on the external IR illuminators when the camera detects low light condition and enters the night mode. This can be done by connecting a pair of DO signals to external IR device, and configuring a DO triggering event via the event setting.

Turn on built-in IR illuminator in night mode
Select this to turn on the built-in IR illuminators (effective range up to 15 meters) when the camera detects low light condition and enters the night mode.

IR cut filter

With a removable IR-cut filter, this Network Camera can automatically remove the filter to allow IR light enter the sensor during low light conditions.

- Auto mode
  The Network Camera automatically removes the filter by judging the level of ambient light.
- Day mode
  In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.
- Night mode
  In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.
- Synchronize with digital input
  The Network Camera automatically removes the IR cut filter when a Digital Input is triggerred. This applies when the camera is installed into a housing that provides its own IR lights and sensor.
- Schedule mode
  The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

Light sensor sensitivity
Select Low, Normal, or High sensitivity for the light sensor.

Image settings

On this page, you can tune the White balance and Image adjustment.

White balance: Adjust the value for the best color temperature.

■ You may follow the steps below to adjust the white balance to the best color temperature.

1. Place a sheet of paper of white or cooler-color temperature color, such as blue, in front of the lens, then allow the Network Camera to automatically adjust the color temperature.
2. Click the **On** button to **Fix current value** and confirm the setting while the white balance is being measured.

■ In the manual mode, you can manually tune the color temperature by pulling the RGain and BGain slide bars.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from 0% to 100%.

■ Contrast: Adjust the image contrast level, which ranges from 0% to 100%.

■ Saturation: Adjust the image saturation level, which ranges from 0% to 100%.

■ Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.

■ Gamma curve: Default is Auto. Yu can also adjust the image sharpness level, which ranges from 0 to 0.45. You may let firmware Optimize your display or select a value to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

Enable 3D Noise reduction

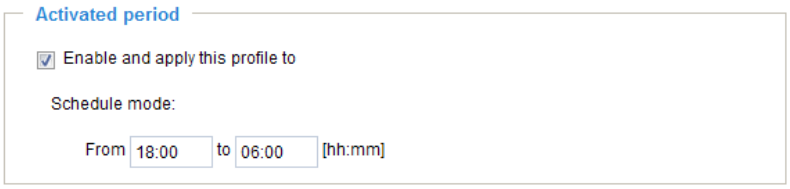
■ Check to enable noise reduction in order to reduce noises and flickers in image. This applies to the onboard 3D Noise Reduction feature. Use the pull-down menu to adjust the reduction strength. Note that applying this function to the video channel will consume system computing power.

3D Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level or disable the function.

Electronic image stabilizer

Select the checkbox to enable the Electronic image stabilization (EIS) function.

Note that the **Preview** button has been cancelled, all changes made to image settings is directly shown on screen. You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting. You can also click on **Profile** to adjust all settings above in a pop-up window for special lighting conditions.



Activated period: Select the mode this profile will apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

Exposure

On this page, you can set the Measurement window, Exposure level, and Exposure mode. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.

Measurement Window: This function allows users to set measurement window(s) for low light compensation.

■ Full view: Calculate the full range of view and offer appropriate light compesation.

IMPORTANT:

1. **When the WDR Pro function is enabled, you cannot enter the Exposure > Manual mode window to configure a measurement window.**
2. **When in the Exposure > Manual setting page, you can configure up to 10 Inclusive measurement windows. There are no Exclusive measurement windows.**
3. **When the WDR Pro function is enabled or disabled, the configuration live view will be temporarily disabled for 8 to 10 seconds.**
4. **If you have different WDR settings in the normal and Profile settings, live view will also be temporarily disabled.**
5. **Trails of after images may occur when large, fast-moving objects appear in the FOV, and when the WDR Pro is enabled.**
6. **When the Electronic image stabilizer is enabled, the live view on the main page will zoom in slightly to a 1.1 ratio.**

■ Custom: This option allows you to manually add a specific window as a measuring area. The measuring window refers to “weighted window“ where the lighting condition within the particular area is taken into account. Camera firmware then adopts the weighted averages method to calculate the value. You can create up to 10 inclusive windows.

■ BLC: When selected, a BLC window will appear on screen meaning that the center of the scene will be taken as a weighed area. This option enables light compensation for images that are too dark or too bright to recognize; for example, for the dark side of objects that is posed against bright sunlight.

Exposure control:

■ **Exposure level**: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright). You can click and drag the pointers on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automatically tune to an optimal imaging result. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

■ **Exposure mode**:

Auto: If you set Exposure mode as **Auto**, the Exposure time and Gain control will not be configurable since the sensor library will automatically adjust the value according to the ambient light. Then you can set iris mode as “indoor” or “outdoor” to reach the best image quality.

■ Iris mode: Select Indoor or Outdoor iris mode to adapt to the installation. The preset iris aperture setting will apply.

Manual: (**Note that some of the Manual options will be disabled when WDR Pro is enabled!**)

■ Iris Adjustment (available in the Manual mode): The camera comes with a P-iris lens, which controls the iris opening with extreme precision by its built-in stepping motor. Via software controls, the lens maintains the iris opening at an optimal level at all times, resulting in superior sharpness and depth of field as well as image quality.

You can manually tune the value of iris opening (aperture size), which can range from 0 (Close. smallest aperture size) to 100 (Open, largest aperture size).

Once set, the iris will stay at current position as long as the lighting condition allows. When external lighting conditions exceed an acceptable range, the P-iris mechanism adjusts itself.

■ Exposure Time: The configurable max. exposure time is tunable according to lighting conditions with values ranging from 1/10000 to 1/5 of a second.

■ Gain Control: Tune the slider bar to set the Gain Control to the best image quality. Higher gain control value will generate a certain amount of noises.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings.

■ **WDR Pro** : When enabled, you can select the strength of the WDR function. The Low, Medium, High options correspond to the level of contrast between the overly-lit area and the shaded areas. For example, the High option applies to a high contrast scenario. Note that when the exposure time is set to longer than 1/60 second, the WDR function will be disabled.

The Sensitivity option applies to the response speed to the change in bright-to-dark lighting contrast.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile of exposure settings page as shown below.

Activated period: Select the mode this profile to apply to the Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

Please follow the steps below to setup a profile:

1. Check **Enable this profile**.
2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose the Schedule mode.
3. Configure Exposure control settings in the folowing columns. Please refer to previous dicussions for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.

Focus

Focus, also known as **Remote Focus**, is applicable to Network Cameras that are equipped with stepping motor lens. The automated focus adjustment function eliminates the needs to physically adjust camera focus. In an outdoor deployment consisting of a large number of cameras, the auto focus function can be very helpful when these cameras become out of focus after days or weeks of operation. And that can easily result from the effects of natural forces, e.g., shrink and expand due to a wide range of operating temperatures and the vibration caused by wind.

.

Below is the procedure to perform the automated Zoom and Focus function:

1. Use the **Zoom** slide bar to find an optimal view of the area of interest where you want to adjust its focus. Click and drag the double-triangle pointer to rapidly adjust the zoom ratio. The **Focus** pointer moves with the Zoom pointer correspondingly.

2. Select from the bottom of the screen whether you want to perform focus adjustment on the **Full view** or within a **Custom** focus window. You can create a custom window and click and drag the window to a desired position on screen.

3. Click to select the **Full-range scan** and/or the **Fully-open iris** checkboxes. When selected, a full-range scan through the camera's entire focal length can take about 30 to 80 seconds. If not, the auto focus scan will only go through the length where optimal focus may occur, and that takes about 15 to 20 seconds. In theory, best results of the auto scan can be acquired when the camera's iris is fully open. The iris fully open checkbox is selected by default.

4. Click on the **Perform auto focus** button, and wait for the scan to complete.

5. After a short while, the clearest image obtained should be displayed and the optimal focus range achieved. Use the arrow marks on the sides to fine-tune the focus if you are not satisfied with the results.

The methodology of using the Resize Buttons at the upper left corner of the streaming window is the same as that on the home page.

Auto Focus:

Click the **Perform auto focus** button for the camera to automatically find the best focus. The process takes about 20 seconds to complete. The Focus pointer will stay at the optimal location on the slide bar.

You may still need to use the arrow marks to fine-tune the focus depending on the live image on your screen. “>” means moving from wide to tele end; and “<” tele to wide.

- **Full-range scan**: If selected, the auto focus scan will be performed throughout the complete range of focus. The full-range scan takes a longer time to complete. A full-range scan usually takes approximately 3 minutes or longer.

- **Fully-open Iris**: By default, this checkbox is selected for performing an auto scan and should provide an optimal scan result.

Focus window:

By default, the optimal focus is found on a full view window. You may designate a custom window within your current field of view to acquire the best focus out of it. However, you can not place a focus window on a distant background, e.g., a hall way that stretches away for 3 meters or farther. Doing so you will not benefit from the Focus window function.

- **Full view**: The focus tuning takes place by referring to the full view.

- **Custom**: You can create a focus window and drag it to a place of interest in your view window. Note that it is recommended to use this function only when you have a solid object in your view window that is showing a consistent color or texture. This function will not take effect if you set the focus window on a distant background.

Privacy mask

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.

■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window.
2. You can use the mouse cursor to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Click on the **Enable privacy mask** checkbox to enable this function.

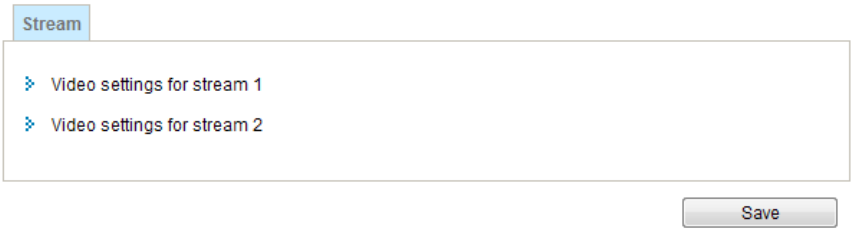
NOTE:

► *Up to 5 privacy mask windows can be set up on the same screen.*

► *If you want to delete the privacy mask window, please click the 'x' on the upper right corner of the window.*

Media > Video

Stream settings



This Network Camera supports multiple streams with frame sizes ranging from

176 x 144 to 1280 x 1024 (IP8355EH)

- or -

176 x 144 to 1920 x1080 (IP8365EH).

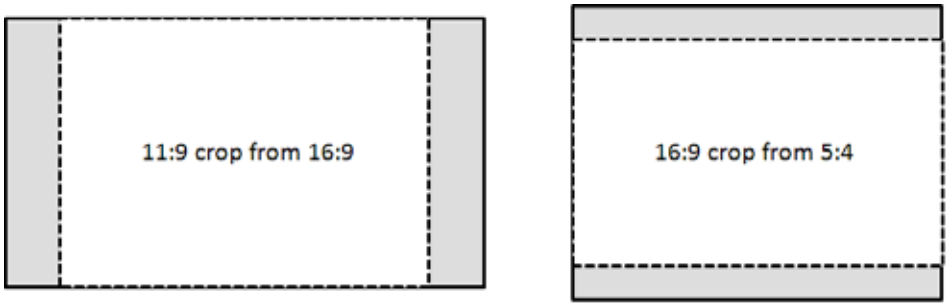
The definition of multiple streams:

■ Stream 1: The default frame size for Stream 1 is set to the 1280 x 1024 at 30fps.

■ Stream 2: The default frame size for Stream 2 is set to the 640 x 480 at 15fps.

IMPORTANT:

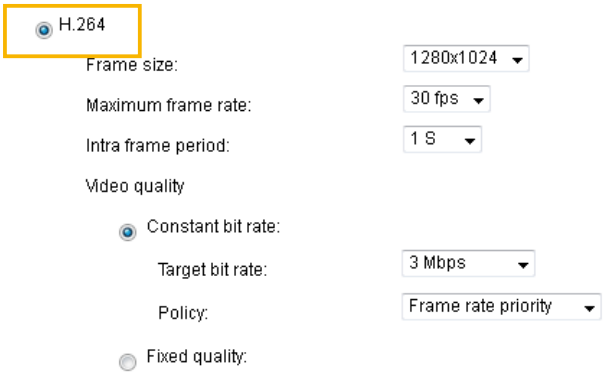
1. **When selecting a different resolution for a video stream, a smaller resolution with a different aspect ratio will be proportionally generated from the original field of view. However, some resolutions, e.g., the 1280x720, has an aspect ratio of 16:9; which is different from the default 5:4 ratio. To maintain the aspect ratio in the display, some areas on the sides of the field of view will be left out.**



2. **The Customized frame rate number is not configurable.**
3. **If manually configuring the Fixed quality value for a video stream using the Customized method, the lowest quality number is 10.**

Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above Viewing Window sections.

This Network Camera offers real-time H.264 and MJPEG compression standards (Dual Codec) for real-time viewing. If the **H.264** mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance:



■ Frame size

You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more network bandwidth.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps.

■ Intra frame period

Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

- Constant bit rate: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, and 8Mbps. You can also select **Customize** and manually enter a value.

  - Target bit rate: select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 8Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.

  - Policy: If Frame rate priority is selected, the Network Camera will try to maintain the frame rate per second performance, while the image quality will be compromised. If Image quality priority is selected, the Network Camera may drop some video frames in order to maintain image quality.

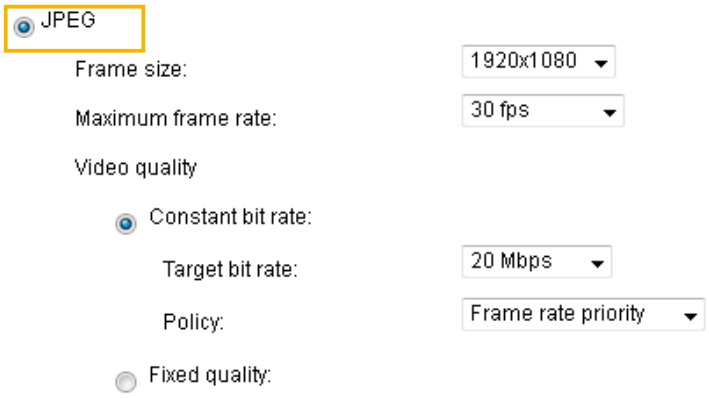
- Fixed quality: On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

  - Maximum bit rate: With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps.

  The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

  You may also manually enter a bit rate number by selecting the **Customized** option.

If **JPEG** mode is selected, the Network Camera sends consecutive JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:



■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. The frame rate will decrease if you select a higher resolution.

■ Video quality
Refer to the previous page setting an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for MPEG4 and H.264.

For Constant Bit Rate and other settings, refer to the previous page for details.

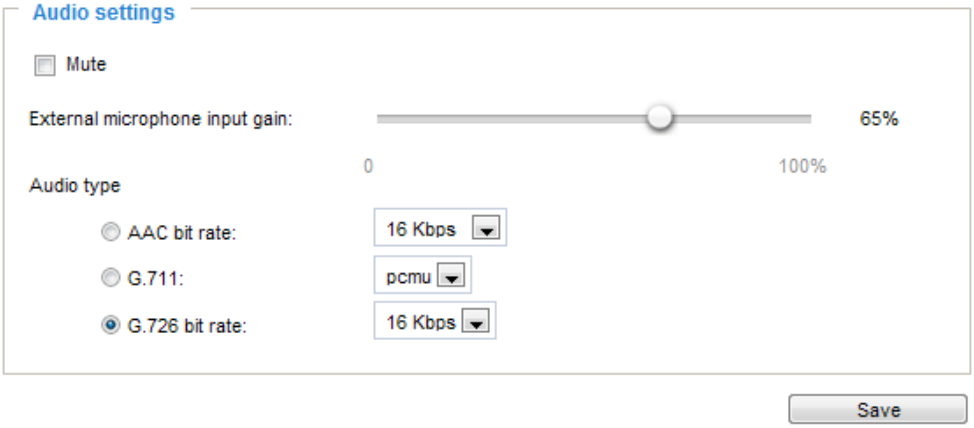
NOTE:

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

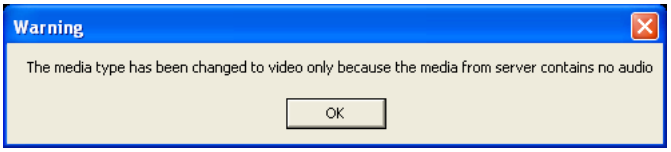
► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Media > Audio

Audio Settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if muted, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



External microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from 100% (most sensitive) to 0% (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.

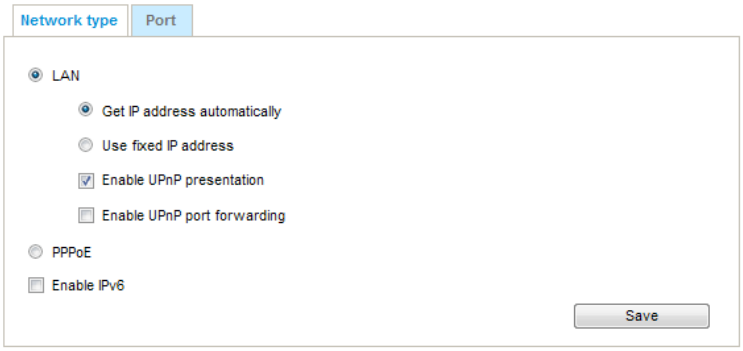
- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

When completed with the settings on this page, click **Save** to enable the settings.

Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

Network Type

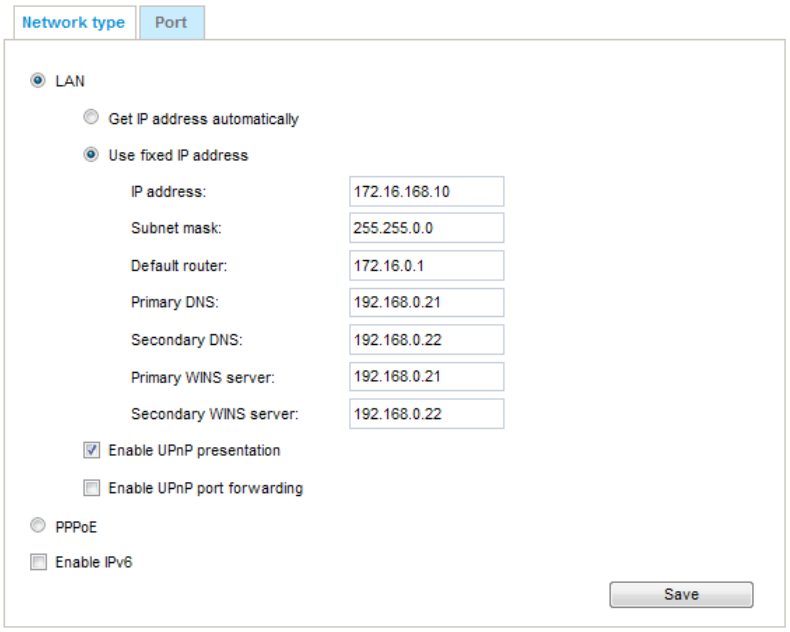


LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Please rememer to click on the **Save** button when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 17 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

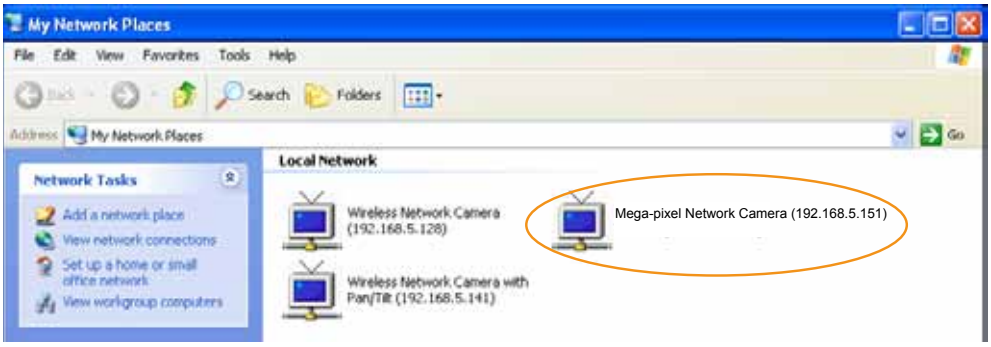
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer names and IP addresses.

Secondary WINS server: The secondary WINS server that maintains the database of computer names and IP addresses.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, the shortcuts to connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



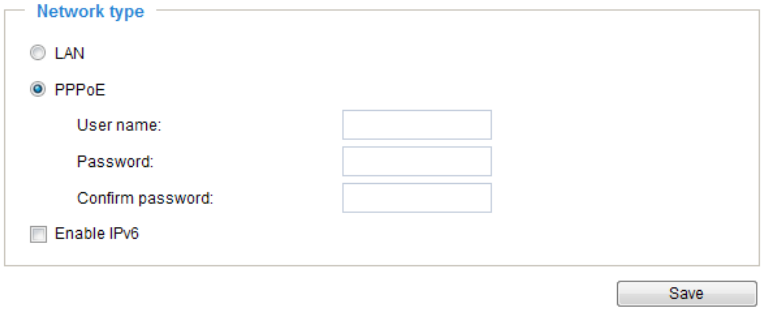
Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 102) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 107).
   Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

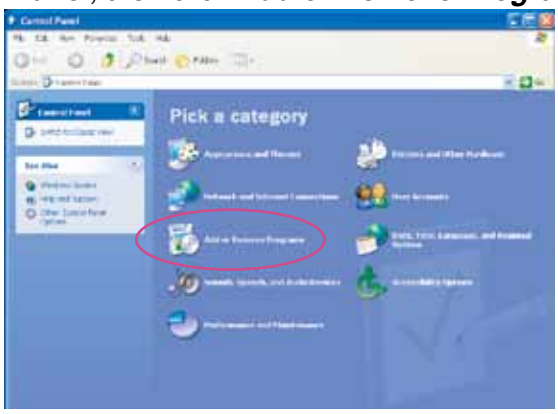
NOTE:

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

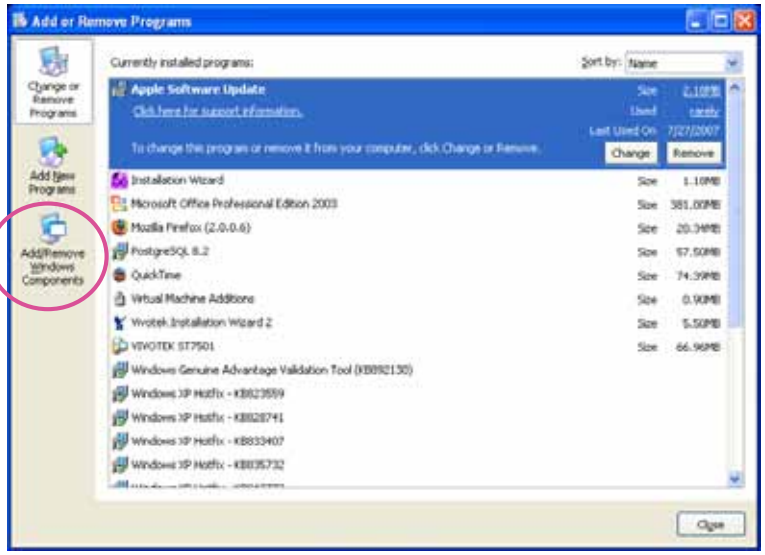
► *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable the UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

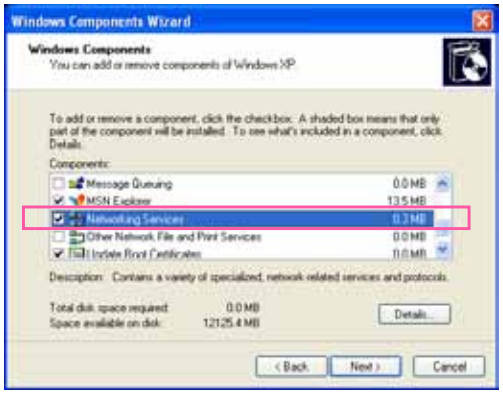
1. *Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



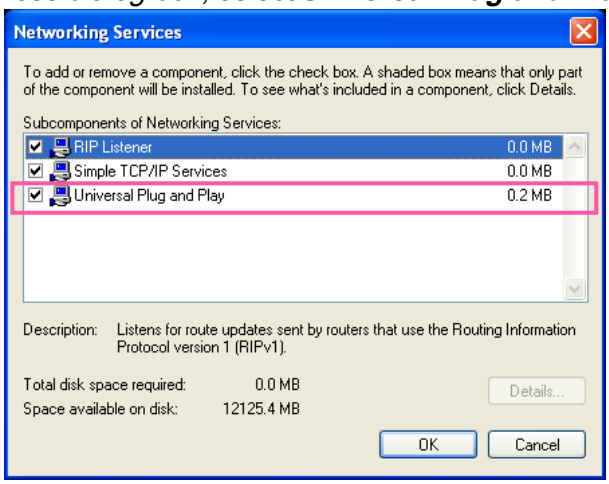
2. *In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



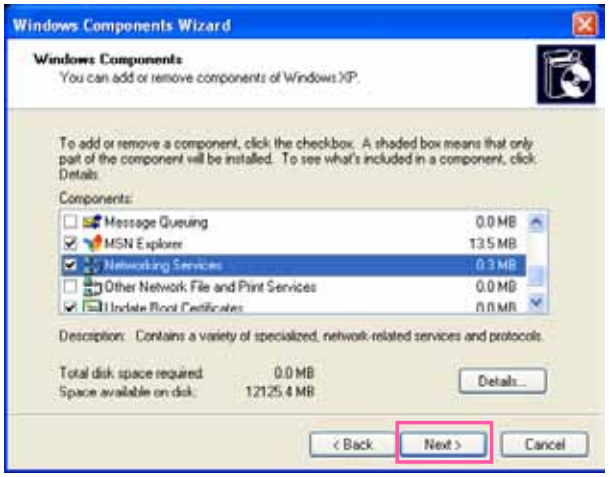
3. *In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing
MSN Explorer
Networking Services
Other Network File and Print Services
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required:
Space available on disk:
Details...
< Back
Next >
Cancel

4. In the Networking Services dialog box, select ***Universal Plug and Play*** and click ***OK***.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).
Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB
Details...
OK
Cancel

5. Click ***Next*** in the following window.


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing 0.0 MB
MSN Explorer 13.5 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB
Details...
< Back
Next >
Cancel

6. Click ***Finish***. *UPnP™ is enabled.*

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

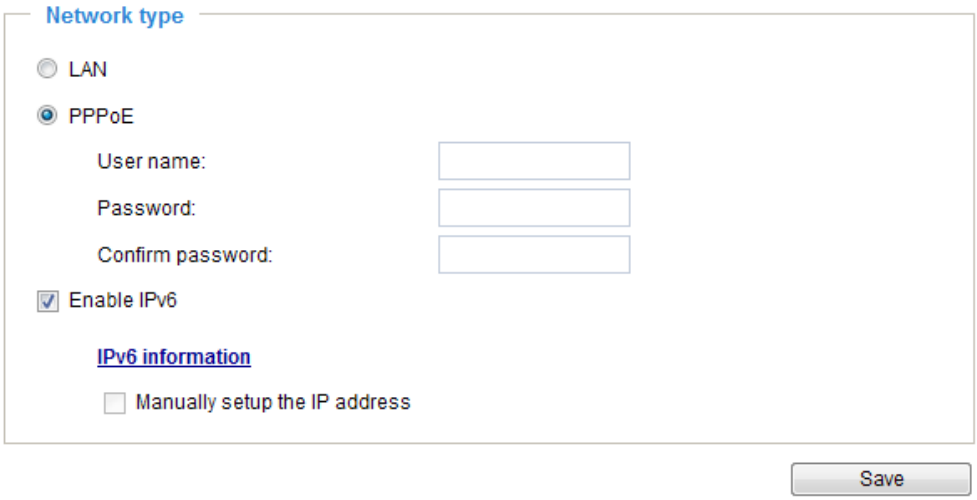
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 45 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

Select the Enable IPv6 checkbox and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 7 or 8, Mozilla Firefox 13.0 or above.

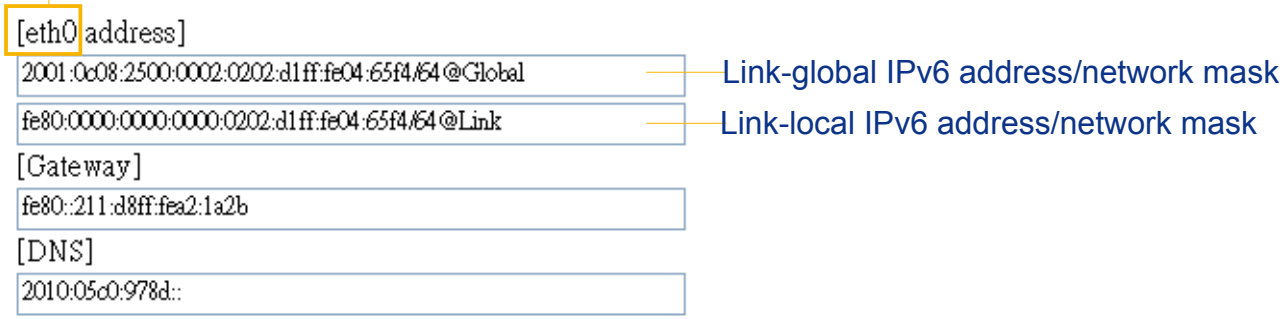


When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

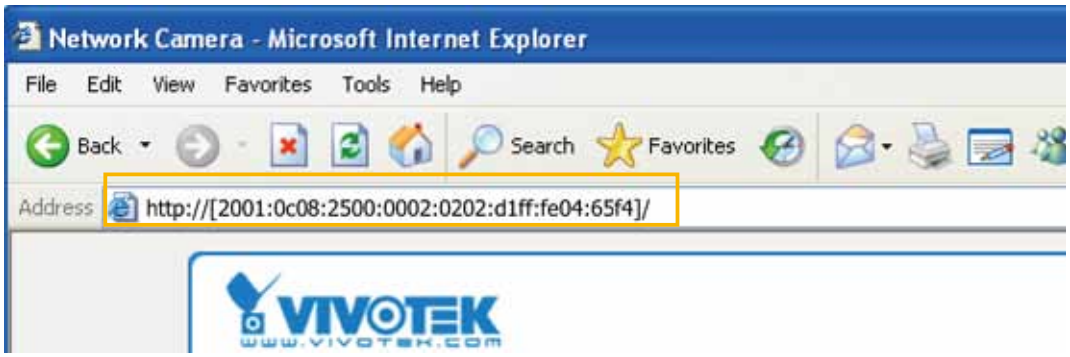
If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

Refers to Ethernet



Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

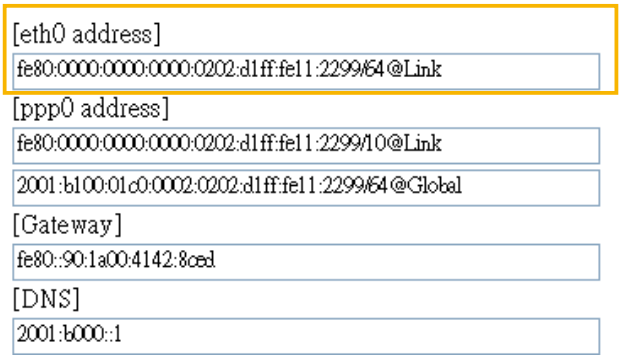
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:



NOTE:

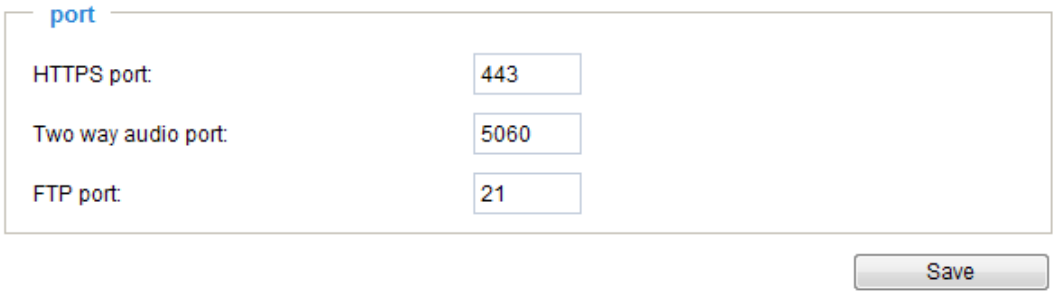
► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage using the following address format: (Please refer to **HTTP** streaming on page 71 for detailed information.)*

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*



Manually setup the IP address: Select this option to manually configure IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. If you check this item, the following blanks will be displayed for you to enter the corresponding information:

Port

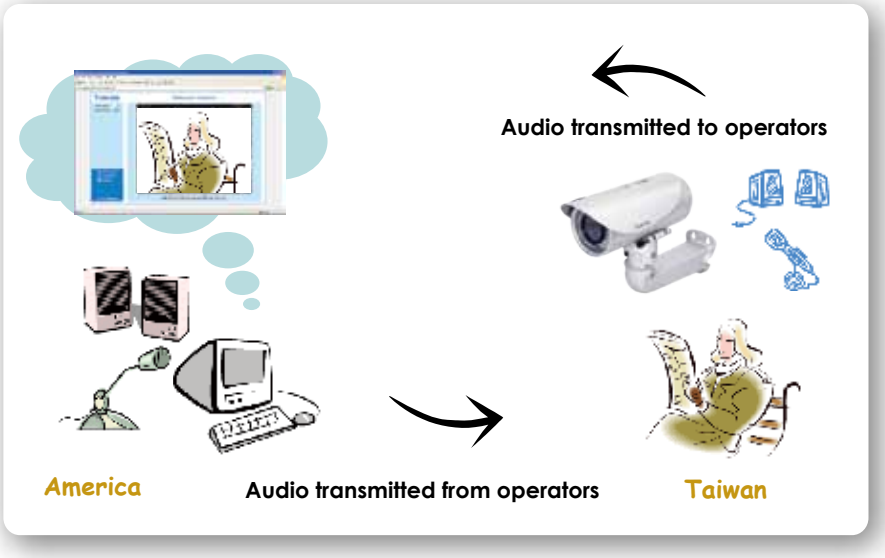


HTTPS port: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio port: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" or "H.264" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 31 and Stream settings on page 58.



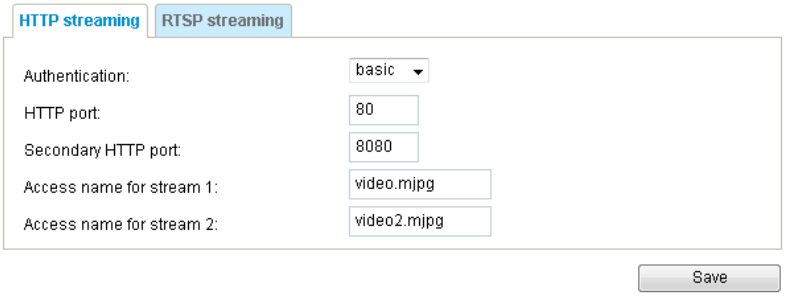
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP port: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

Network > Streaming protocols

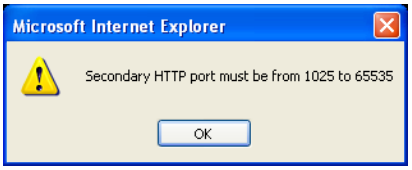
HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 81 for details.



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

On the LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 ~ 2: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 58.

When using **Mozilla Firefox** to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox.

URL command -- http://<ip address>:<http port>/<access name for stream 1~2>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

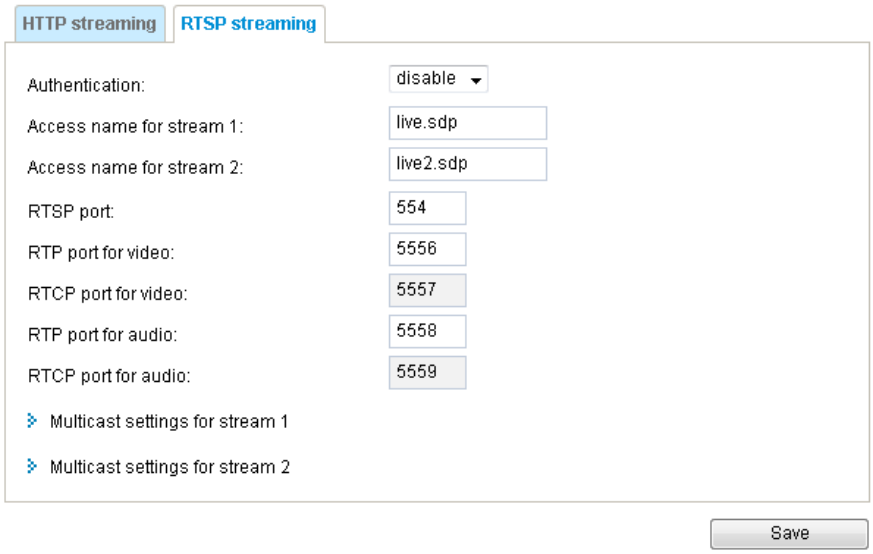
video2.mjpg (JPEG Image, 320x240 pixels) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.5.151/video2.mjpg
Google
Customize Links Free Hotmail Windows Media Windows

NOTE:

► *Microsoft® Internet Explorer does not support server push technology; therefore, you will not be able to access a video stream using http://<ip address>:<http port>/<access name for stream 1~2> .*

RTSP Streaming

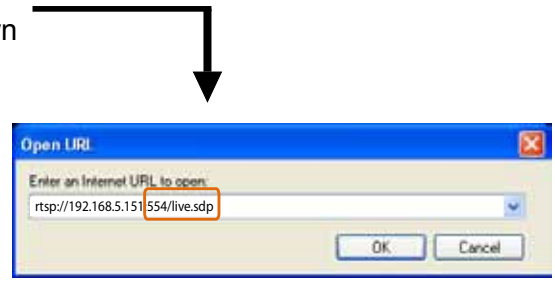
To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 81 for details.


HTTP streaming
RTSP streaming
Authentication: disable
Access name for stream 1: live.sdp
Access name for stream 2: live2.sdp
RTSP port: 554
RTP port for video: 5556
RTCP port for video: 5557
RTP port for audio: 5558
RTCP port for audio: 5559
Multicast settings for stream 1
Multicast settings for stream 2
Save

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed below:

	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 ~ 2: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.

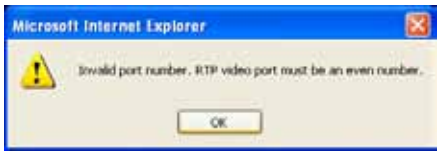


RTSP port /RTP port for video and RTCP port for video

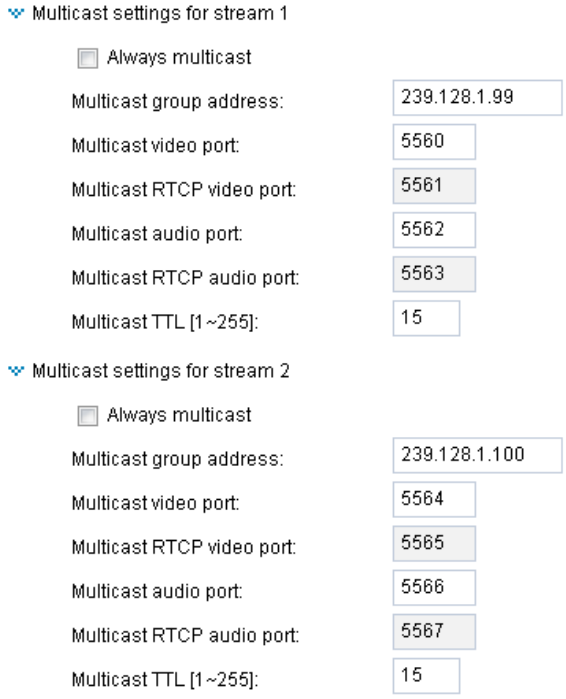
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 5556.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:



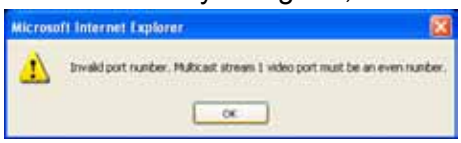
Multicast settings for stream 1 ~ 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 2.


Multicast settings for stream 1
Always multicast
Multicast group address: 239.128.1.99
Multicast video port: 5560
Multicast RTCP video port: 5561
Multicast audio port: 5562
Multicast RTCP audio port: 5563
Multicast TTL [1~255]: 15
Multicast settings for stream 2
Always multicast
Multicast group address: 239.128.1.100
Multicast video port: 5564
Multicast RTCP video port: 5565
Multicast audio port: 5566
Multicast RTCP audio port: 5567
Multicast TTL [1~255]: 15

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

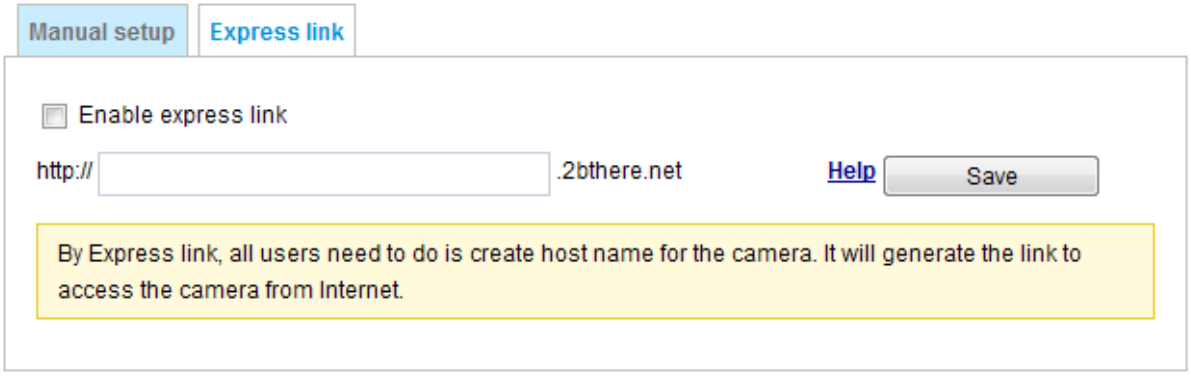
Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

Network > DDNS

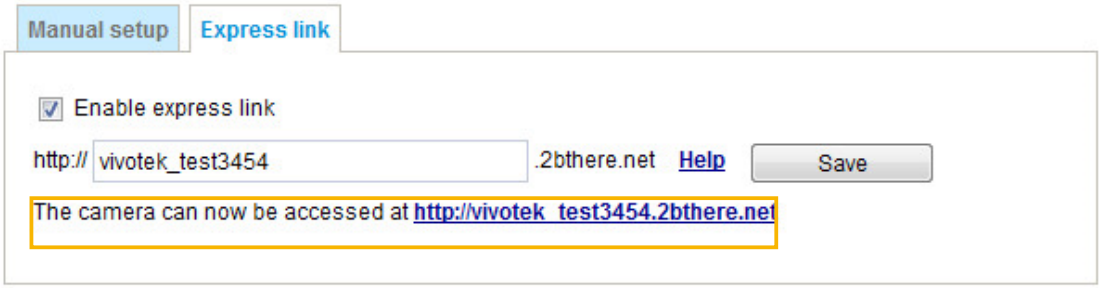
This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

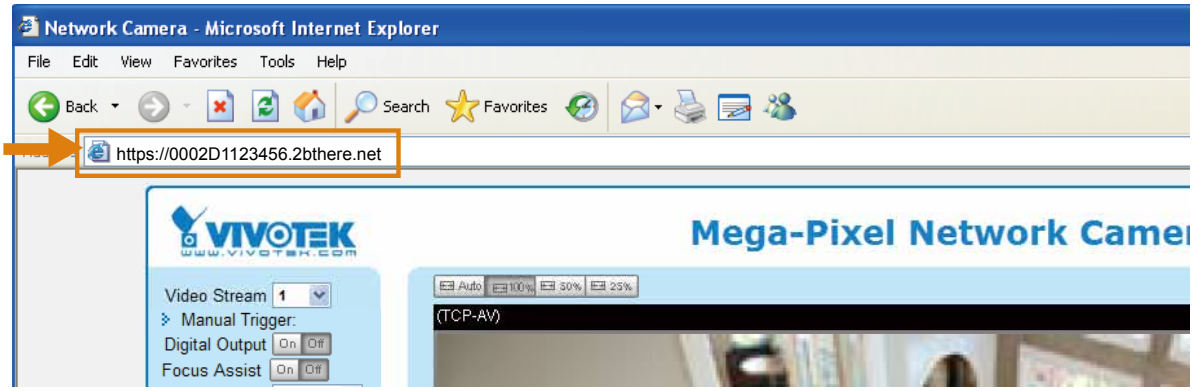
Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.


Manual setup
Express link
Enable express link
http://
.2bthere.net
Help
Save
By Express link, all users need to do is create host name for the camera. It will generate the link to access the camera from Internet.

Please follow the steps below to enable Express Link:
1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will display a message as shown below.





Manual setup

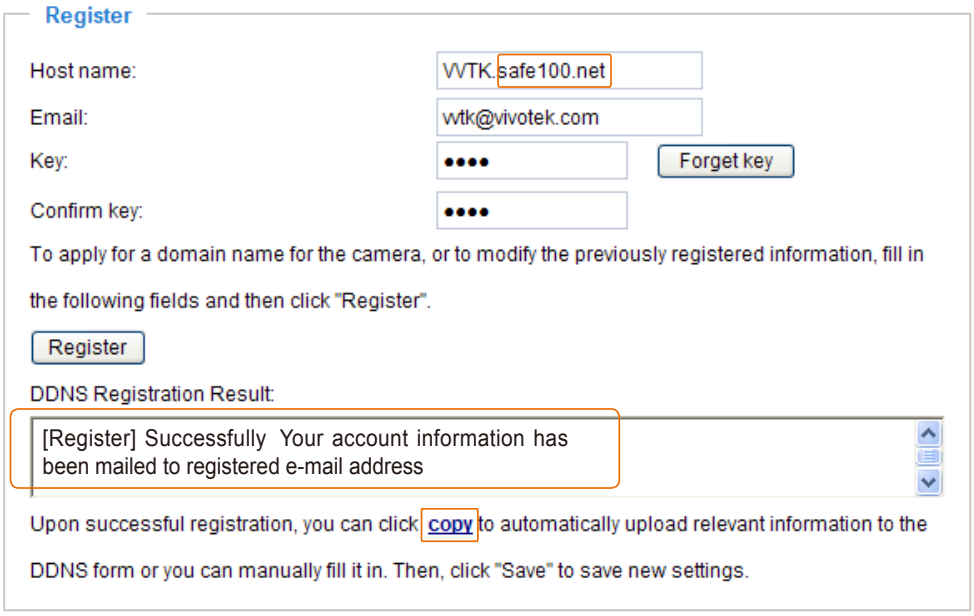
DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.

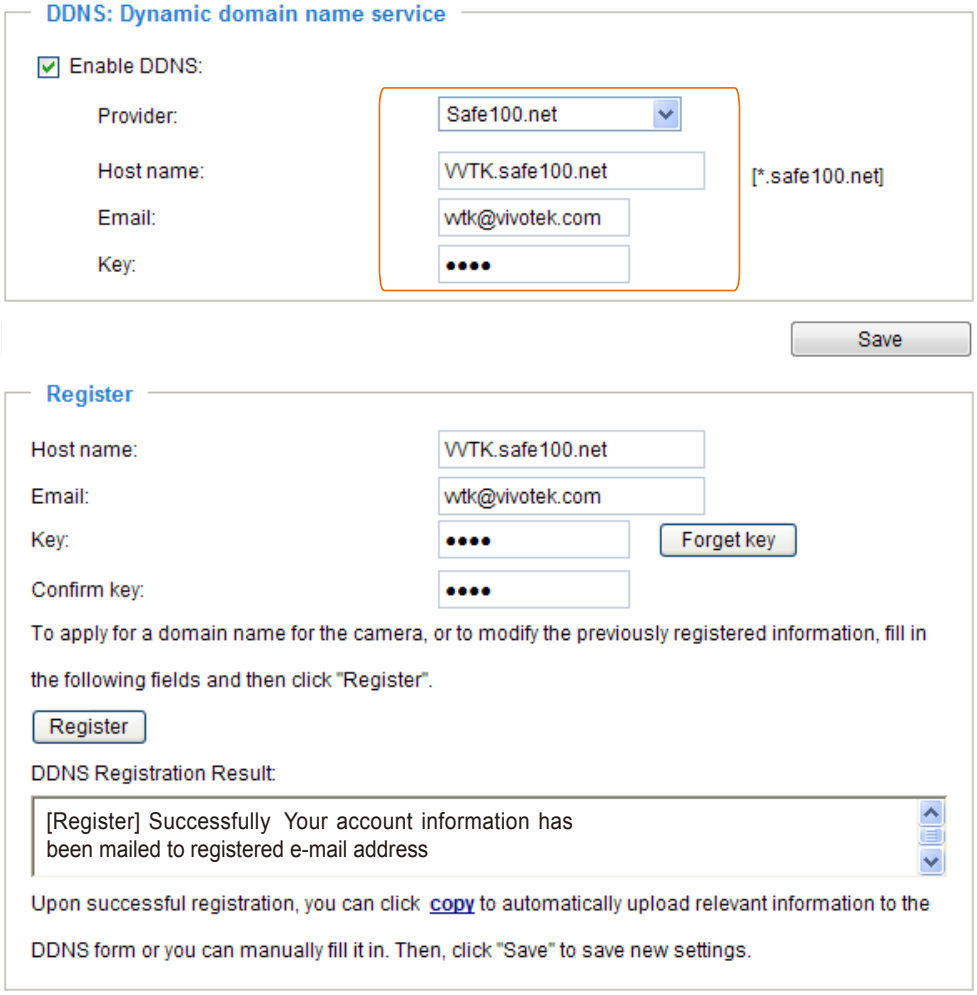
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), CustomSafe100, and dyn-interfree.it. Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.


Register
Host name:
VVTK.safe100.net
Email:
vvtk@vivotek.com
Key:
Forget key
Confirm key:
To apply for a domain name for the camera, or to modify the previously registered information, fill in
the following fields and then click "Register".
Register
DDNS Registration Result:
[Register] Successfully Your account information has
been mailed to registered e-mail address
Upon successful registration, you can click copy to automatically upload relevant information to the
DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.


DDNS: Dynamic domain name service
Enable DDNS:
Provider:
Safe100.net
Host name:
VVTK.safe100.net
[*.safe100.net]
Email:
vtk@vivotek.com
Key:
Save
Register
Host name:
VVTK.safe100.net
Email:
vtk@vivotek.com
Key:
Forget key
Confirm key:
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".
Register
DDNS Registration Result:
[Register] Successfully Your account information has been mailed to registered e-mail address
Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Server name, Email, Key, and Confirm Key; then click **Register**.

   Enter “ns1.safe100.net” as the Server name.

   After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > QoS (Quality of Service)

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

If you assign Video the highest level, the switch will handle video packets first.

NOTE:

► *A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.*

► *The Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

Network > SNMP (Simple Network Management Protocol)

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

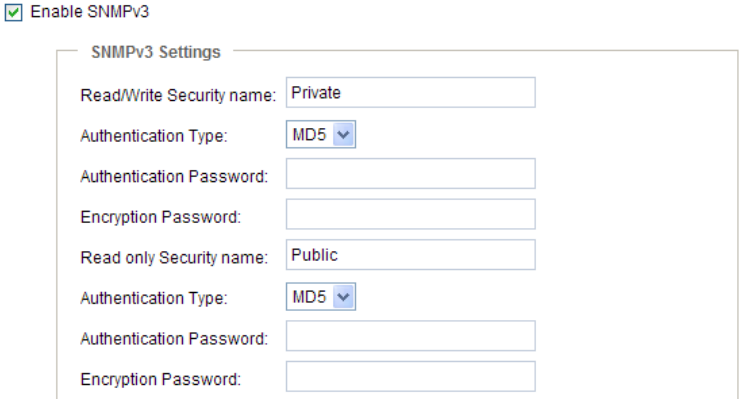
Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

■ Encryption password: Enter a password for encryption (at least 8 characters).



Security > User Account

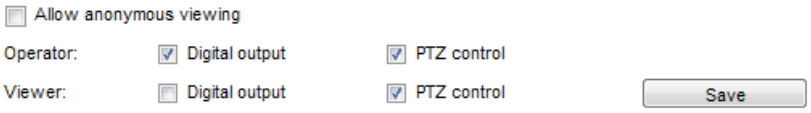
This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

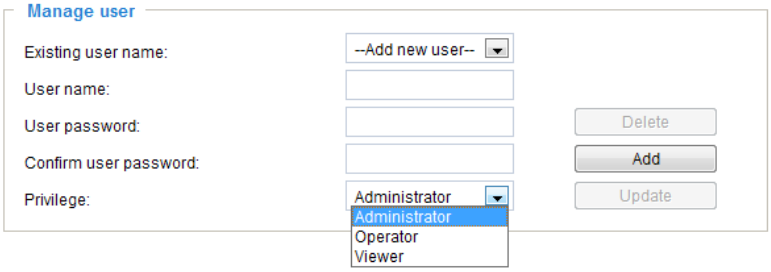
Privilege Management



Digital Output & PTZ control: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 35).

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Manage User



Administrators can add up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 129. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL)

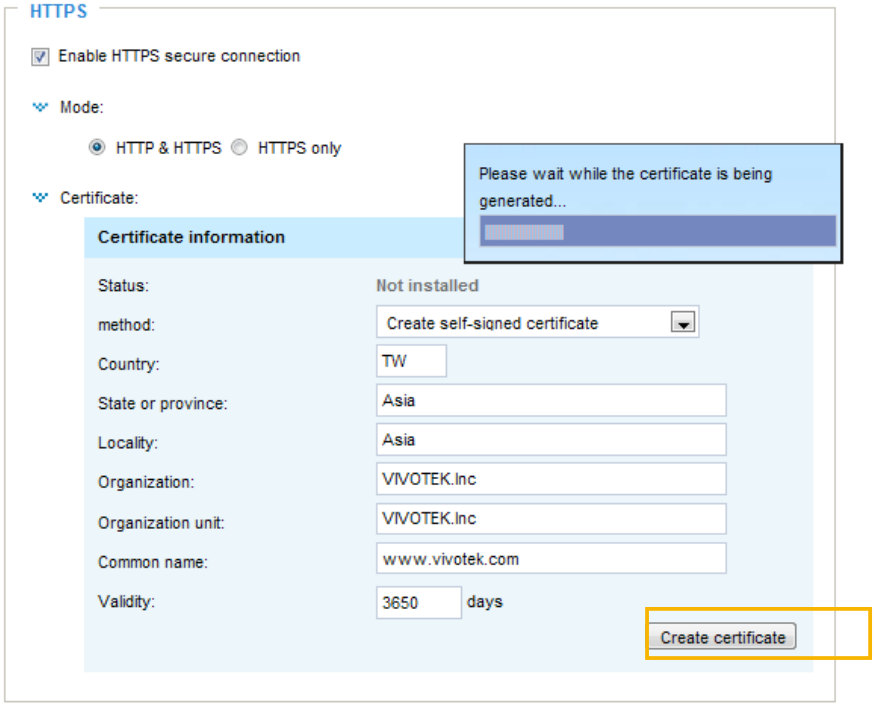
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

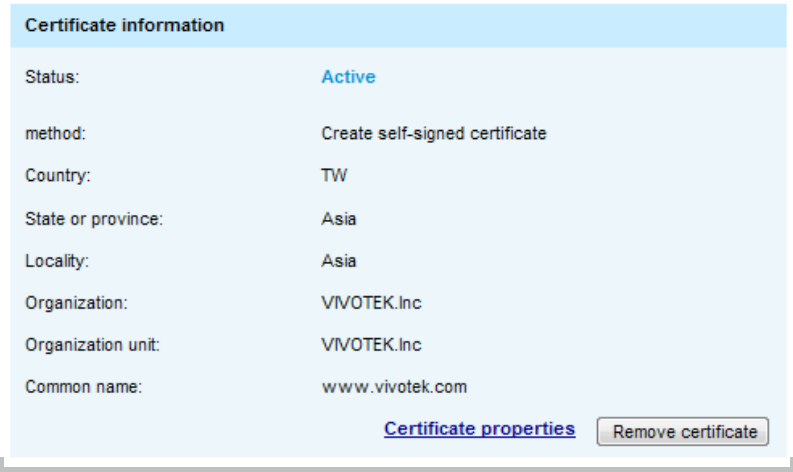
Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate

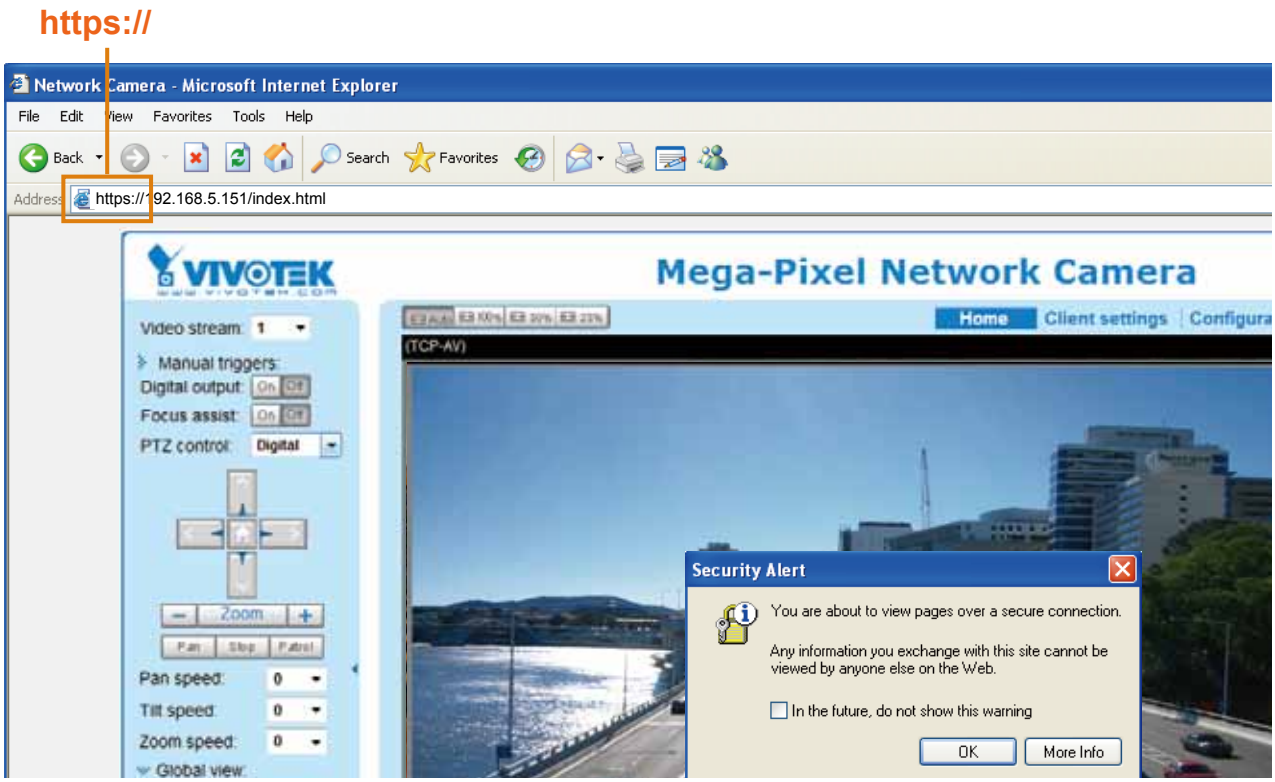
1. Select this option from a pull-down menu.
2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Create certificate** to generate a certificate.



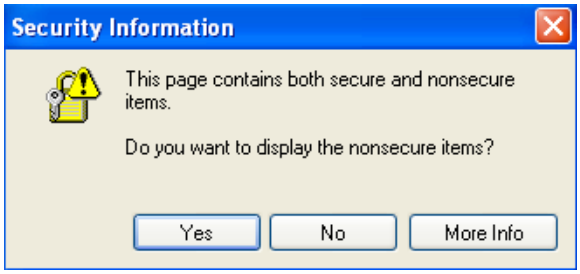
4. The Certificate Information will automatically be displayed as shown below. You can click **Certificate properties** to view detailed information about the certificate.



5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

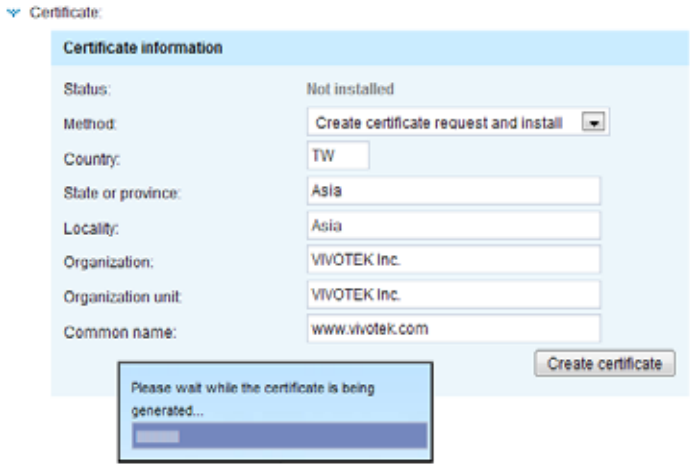


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

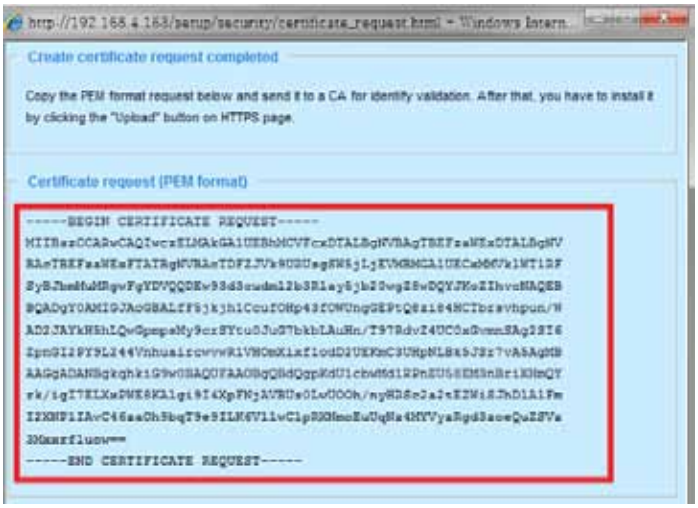


Create certificate request and install

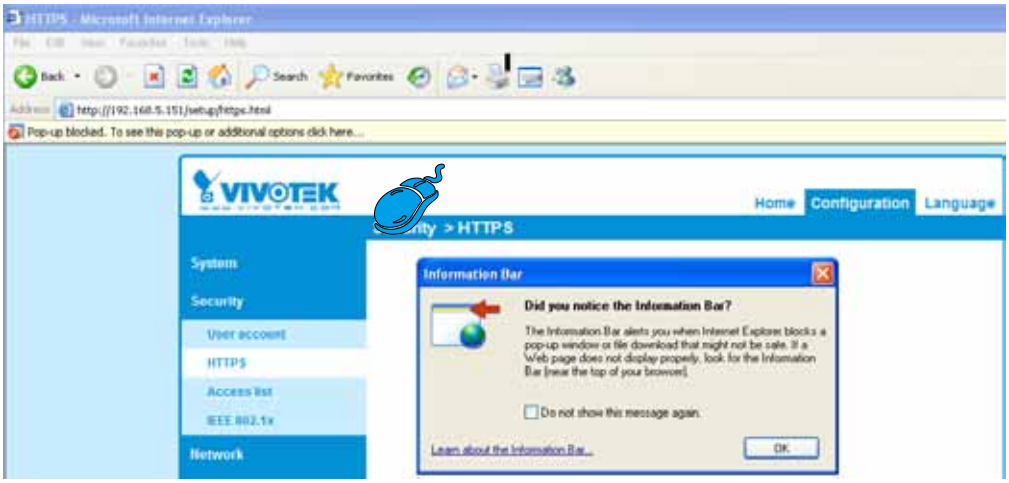
1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.



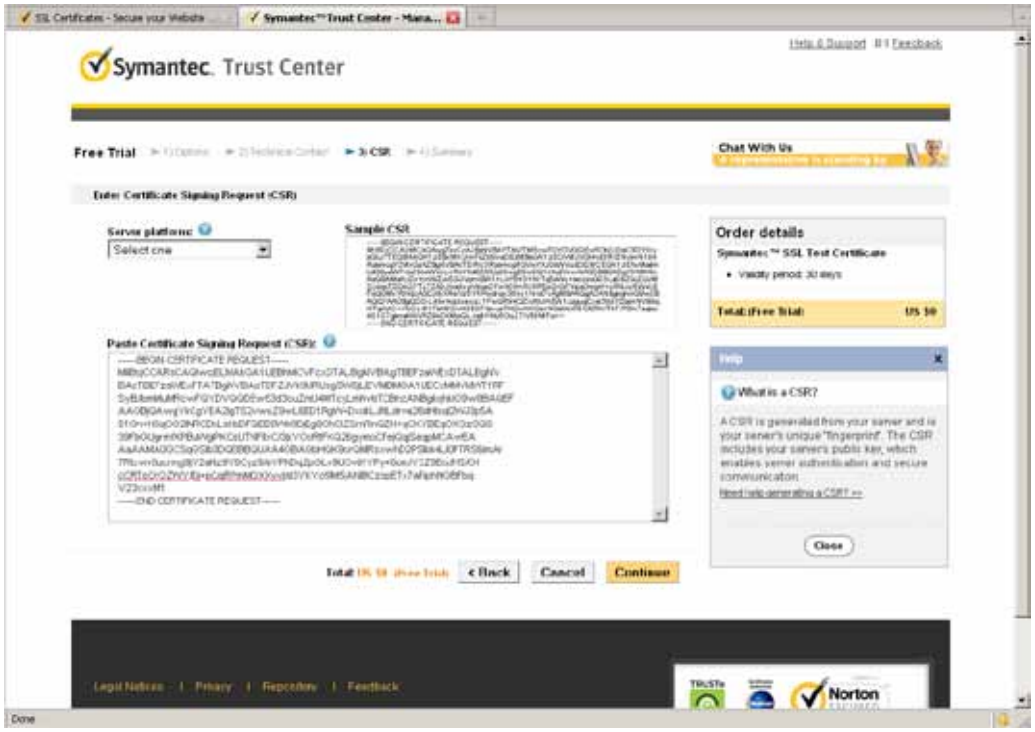
4. The Certificate request window will prompt.


Create certificate request completed
Copy the PEM format request below and send it to a CA for identity validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.
Certificate request (PEM format)
-----BEGIN CERTIFICATE REQUEST-----
-----END CERTIFICATE REQUEST-----

If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.



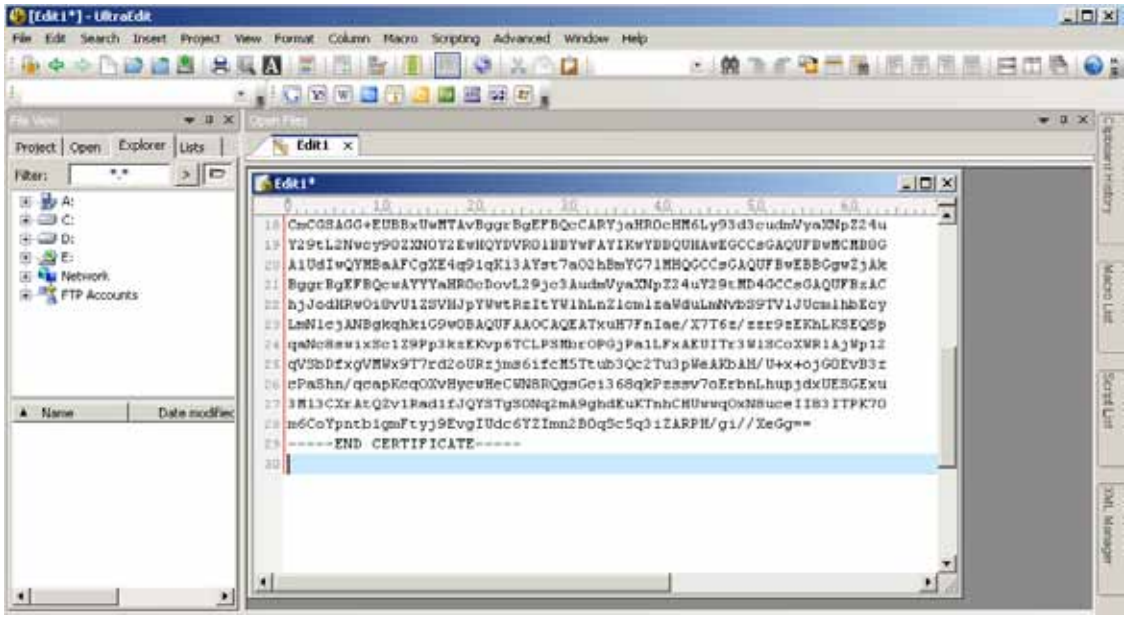
5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.



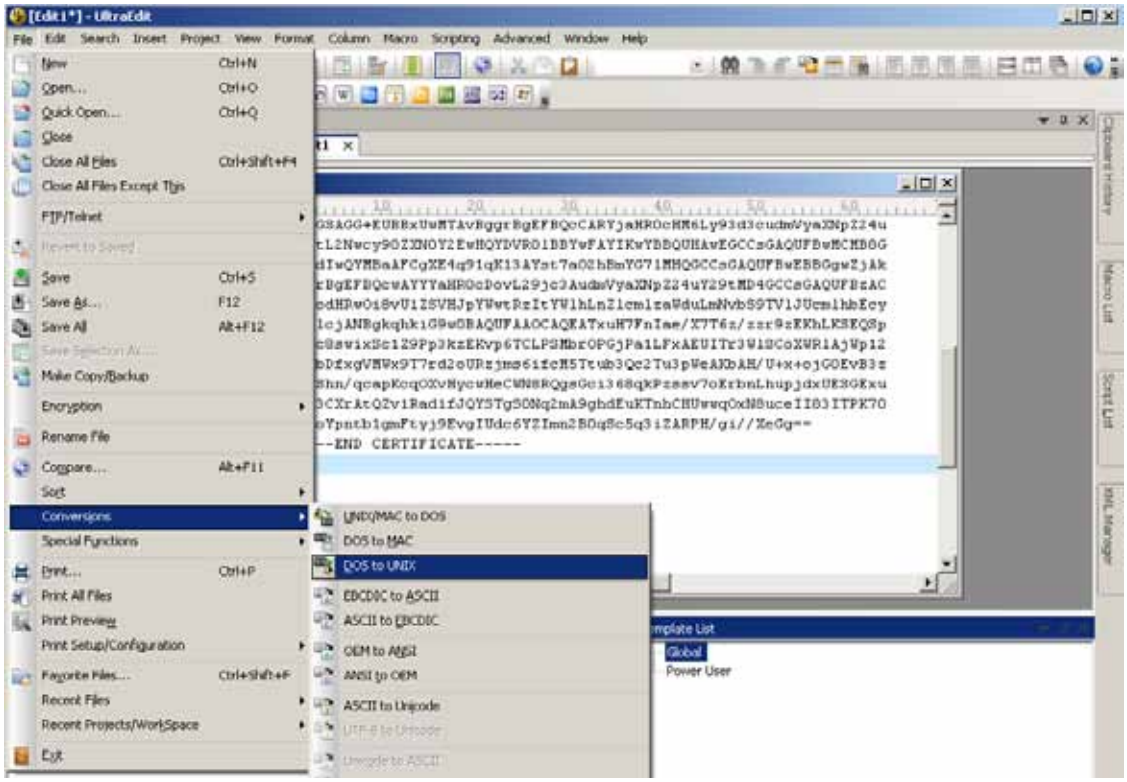
6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com
Thank you for your interest in Symantec!
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

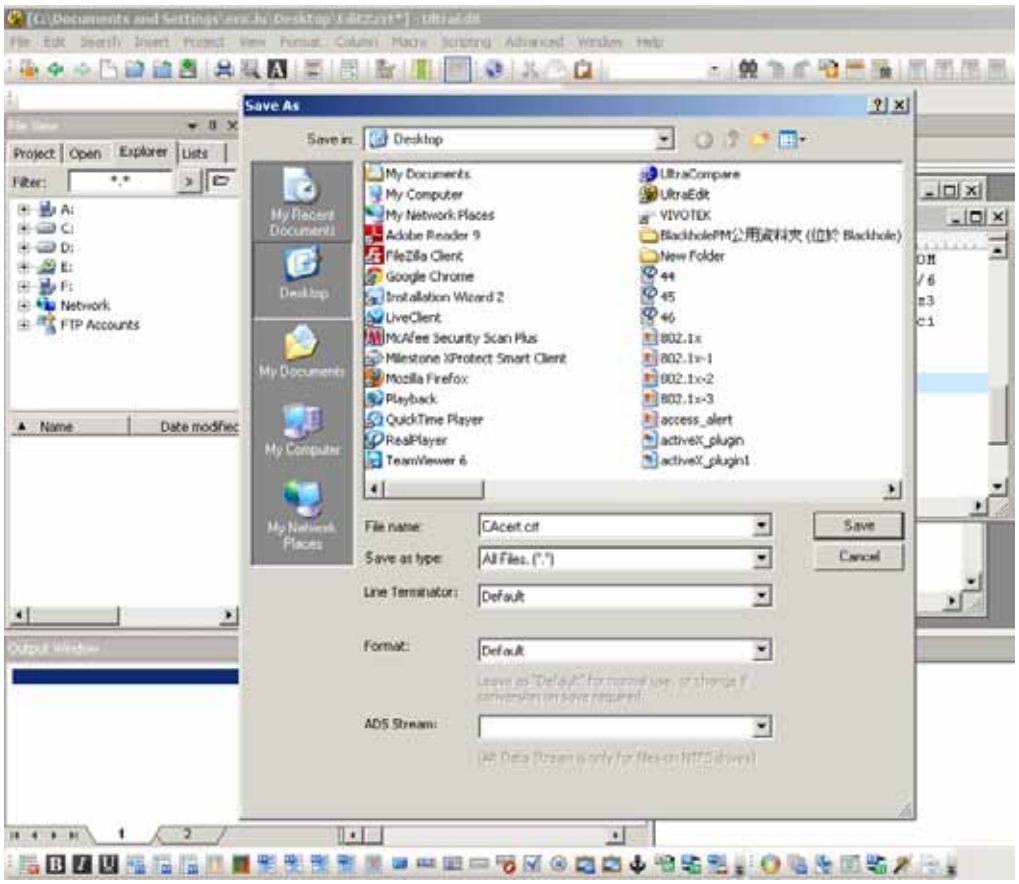
7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.



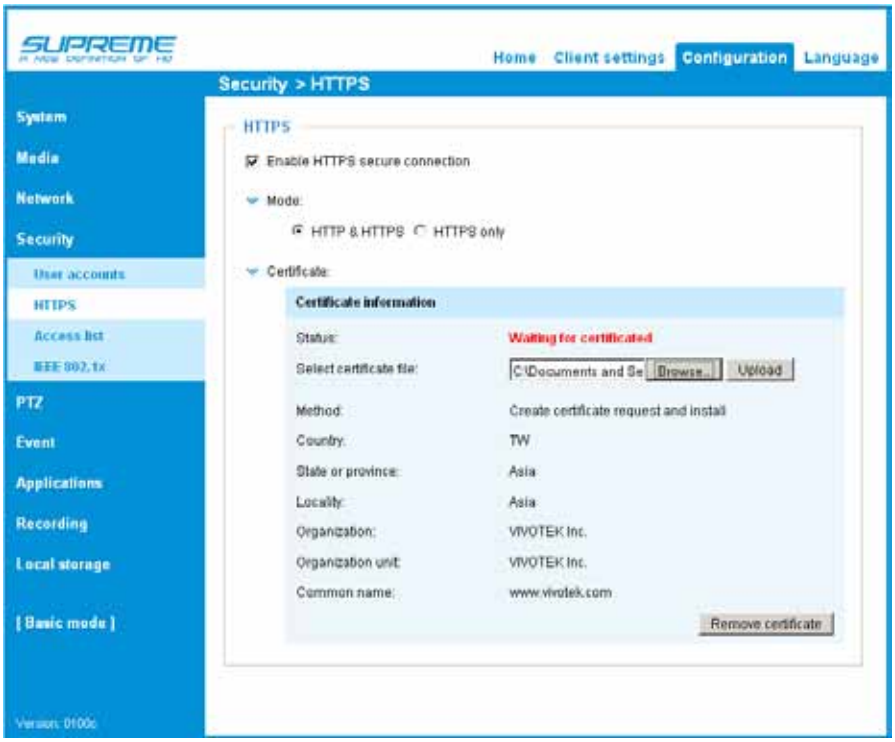
8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.



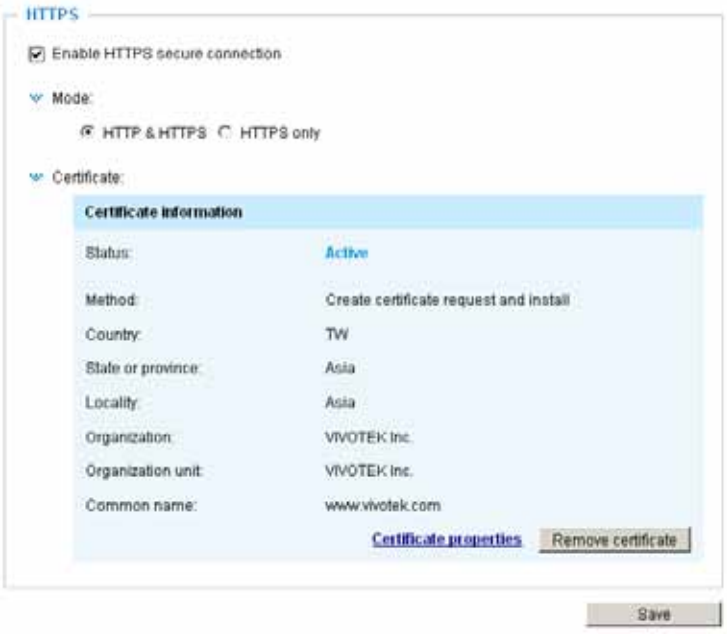
9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."



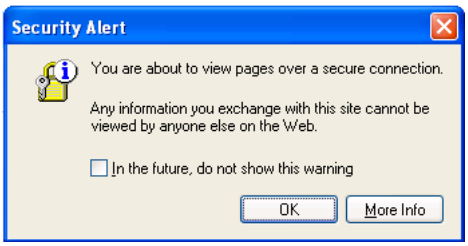
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

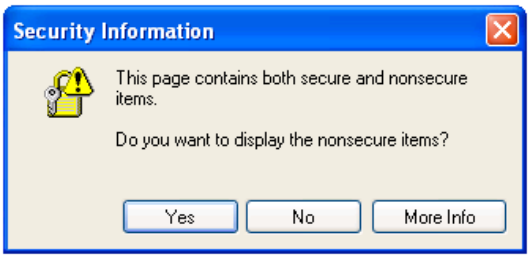


11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the "**Save**" button for the configuration to take effect.



12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.


Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info

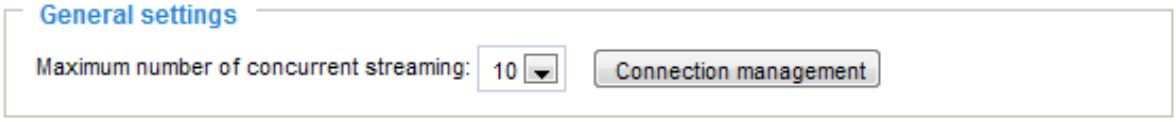


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Security > Access List

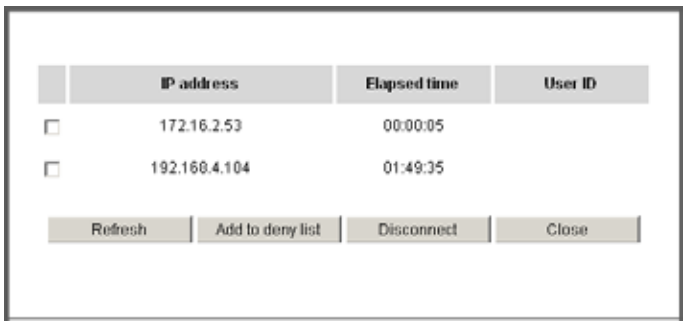
This section explains how to control access permission by verifying the client PC's IP address.

General Settings



Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

Connection management: Click this button to display the connection status window showing a list of the current connections. For example:



Note that only consoles that are currently displaying live streaming will be listed in the Connection management list.

■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations that allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 81.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 72.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 81.

■ Refresh: Click this button to refresh all current connections.

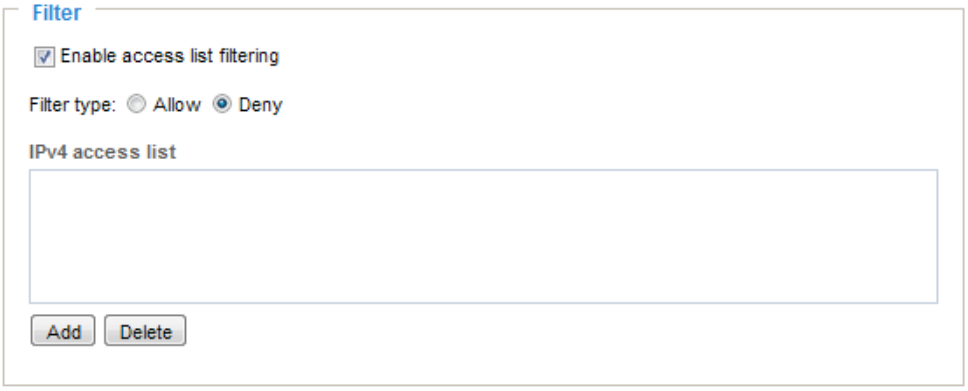
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

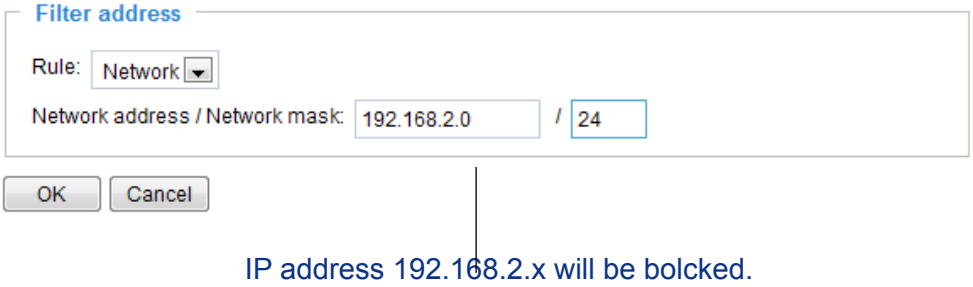
Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.



Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > General settings on page 63 for detailed information.

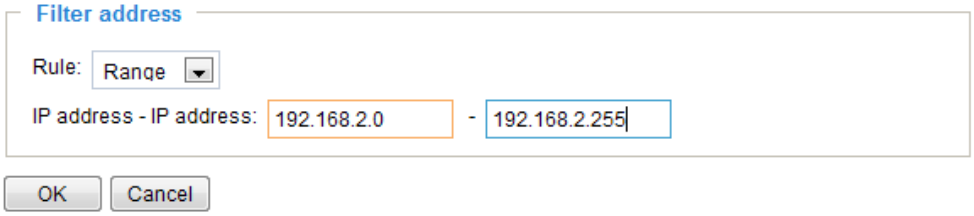
There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format.
For example:



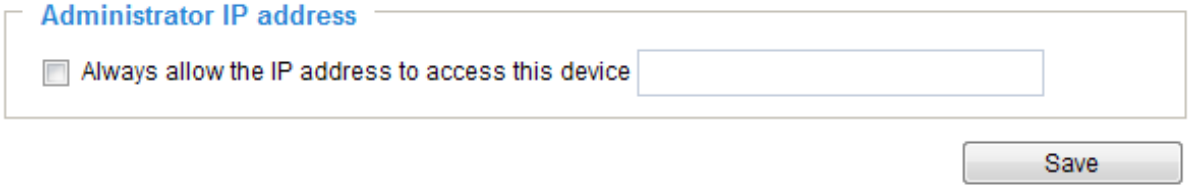
If IPv6 filter is preferred, you will be prompted by the following window. Enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule is only applied to IPv4.
For example:



Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



Security > IEEE 802.1X

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

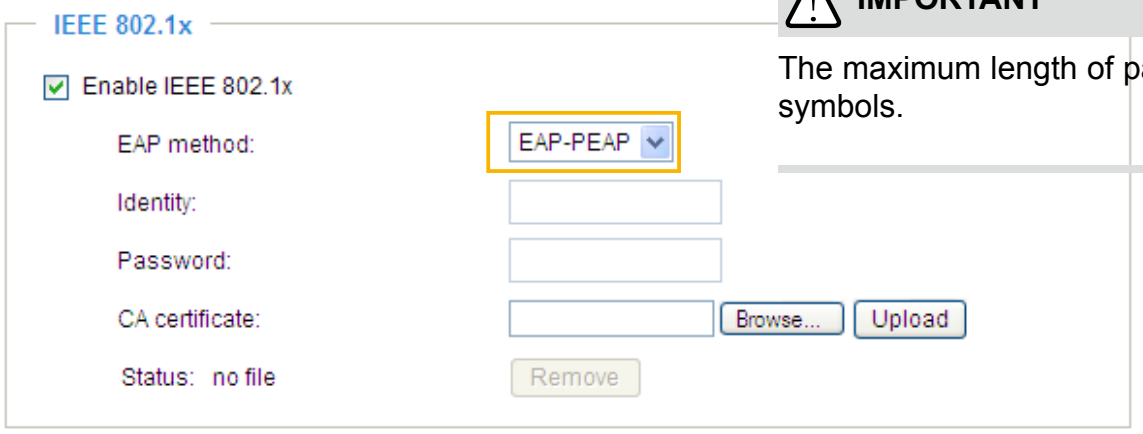
Supplicant (Network Camera) | Authenticator (Network Switch) | Authentication Server (RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

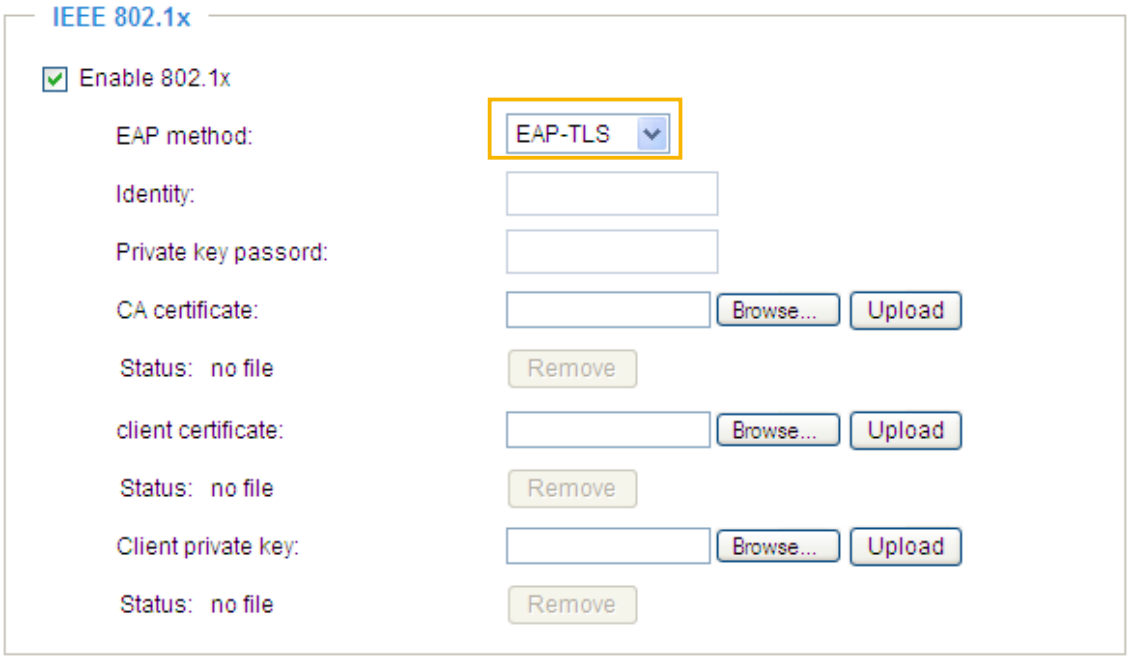
Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).



IMPORTANT

The maximum length of password is 200 symbols.

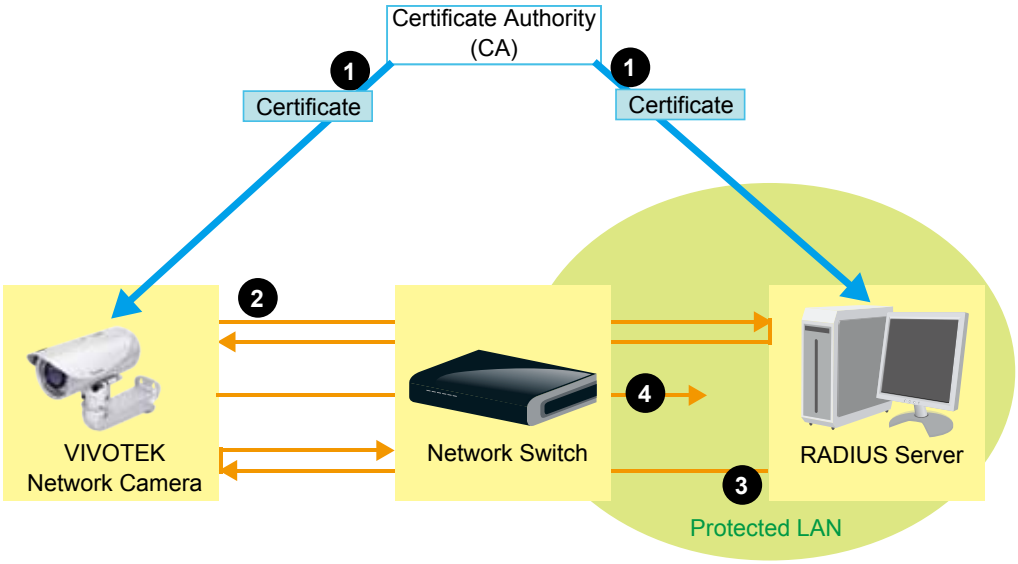


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE:

► *The authentication process for 802.1x:*

1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*

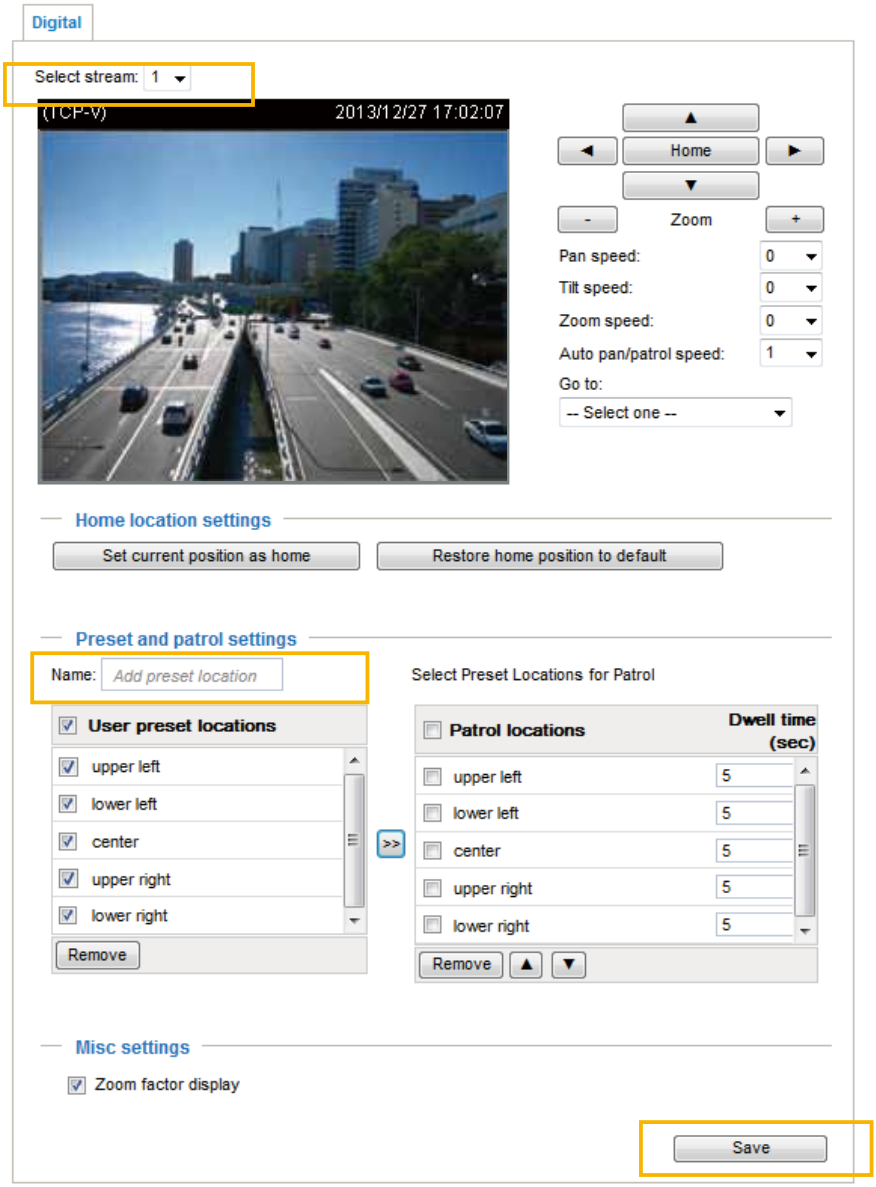


PTZ > PTZ settings

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.
The e-PTZ fucntion allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera. Please refer to below for detailed instruction.

Digital PTZ Operation (E-PTZ Operation)

If you select "Digital", the e-PTZ control settings section will be displayed as shown below:



Set current position as home: If you zoom in on a live view to display only a focused position of the screen, you can use the arrow buttons on the PTZ panel to move the current field of view to a place you preferred, and set it as the home position.

Restore home position to default: This button cancels the previous home position, and returns the field of view to the system default (usually the center of FOV).

Select Stream: Select stream #1 to set up the e-PTZ control. Please note that each stream can possess its own preset and patrol settings. For detailed information about how to set up preset and patrol settings, please refer to page 94.

Auto pan/patrol speed: Select the speed from 1~5 (slow/fast) to set up the Auto pan/patrol speed control.

When completed with the e-PTZ settings, click **Save** to enable the settings on this page.

Home page in E-PTZ Mode

- The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected e-preset position.

- If you have set up different e-preset positions for different streams, you can select one of the video streams to display its separate e-preset positions.

Global View

In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

Moving Instantly

If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame. If deselected, the process moving from one point to the other will be shown, yet it is not easy to observe if the move is not over a long distance.

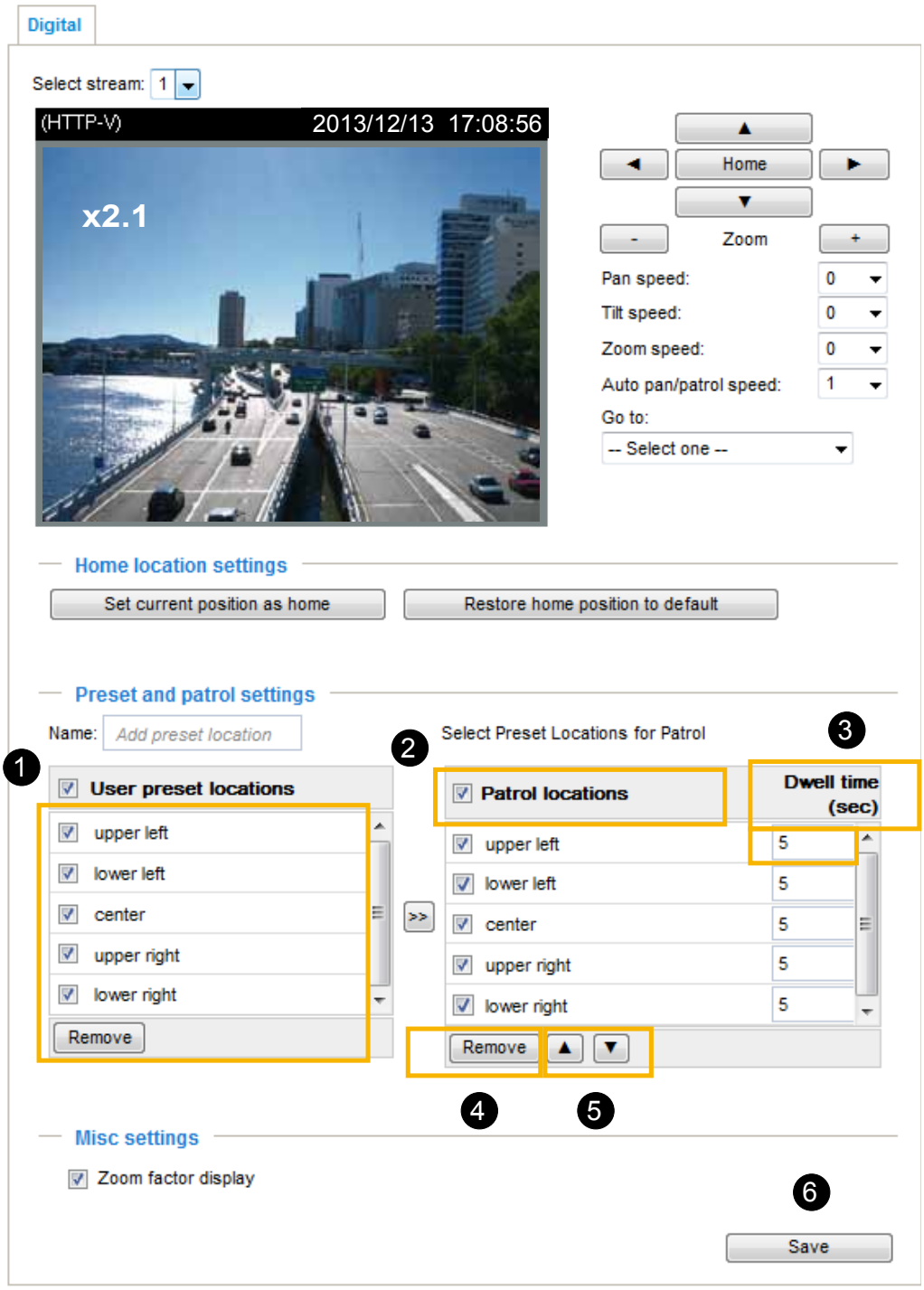
Click on Image

The e-PTZ function also supports “Click on Image“. When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point. Note that the”**Click on Image**” function only applies when you have configured a smaller “Region of Interest” out of the maximum output frame! e.g., a 800x600 region from the camera’s 1280x800 maximum frame size.

Patrol settings

You can select some preset positions for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

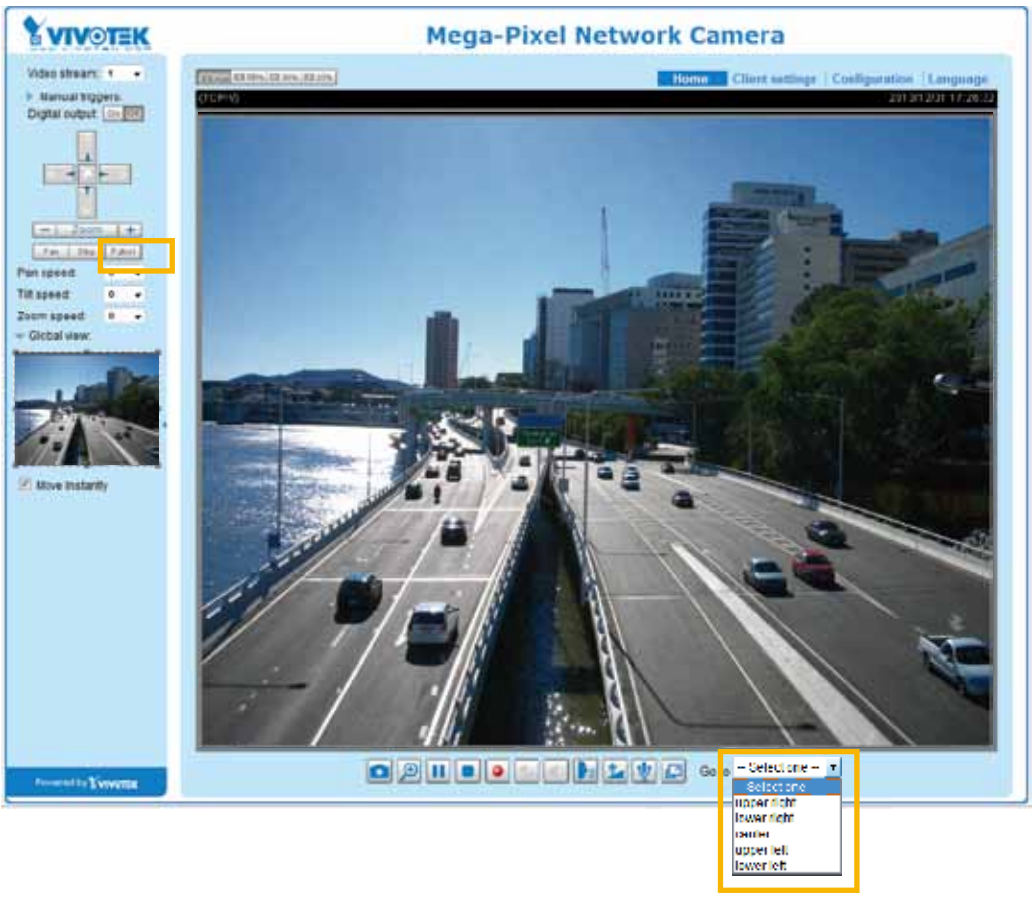
1. Select the preset locations on the list, and click >>.
2. The selected preset locations will be displayed on the **Patrol locations** list.
3. Set the **Dwelling time** for the preset location during auto patrol.
4. If you want to delete a preset location from the Patrol locations list, select it and click **Remove**.
5. Select a location and click ▲ ▼ to rearrange the patrol order.
6. Select patrol locations you want to save in the list and click **Save** to enable the patrol settings.
7. To implement the patrol schedule, please go to homepage and click on **Patrol** button. Please refer to the next page.



Home page in the e-PTZ Mode

The **Preset positions** will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected preset position.

Patrol button: Click this button, then the Network Camera will patrol among the selected preset positions continuously.



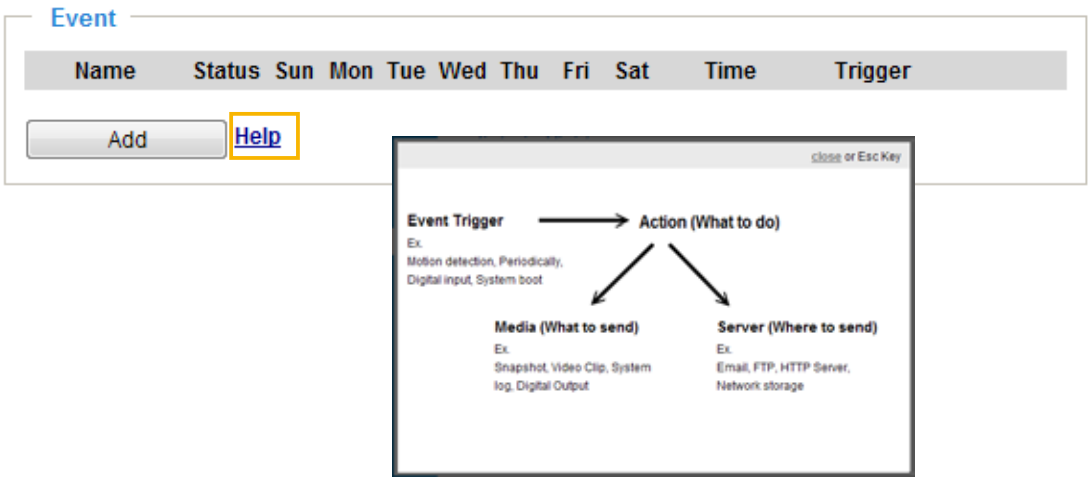
NOTE:

► *The Preset Positions will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected preset position.*

► *Click Patrol: The Network Camera will patrol along the selected positions repeatedly. Please refer to page 96 to see more details.*

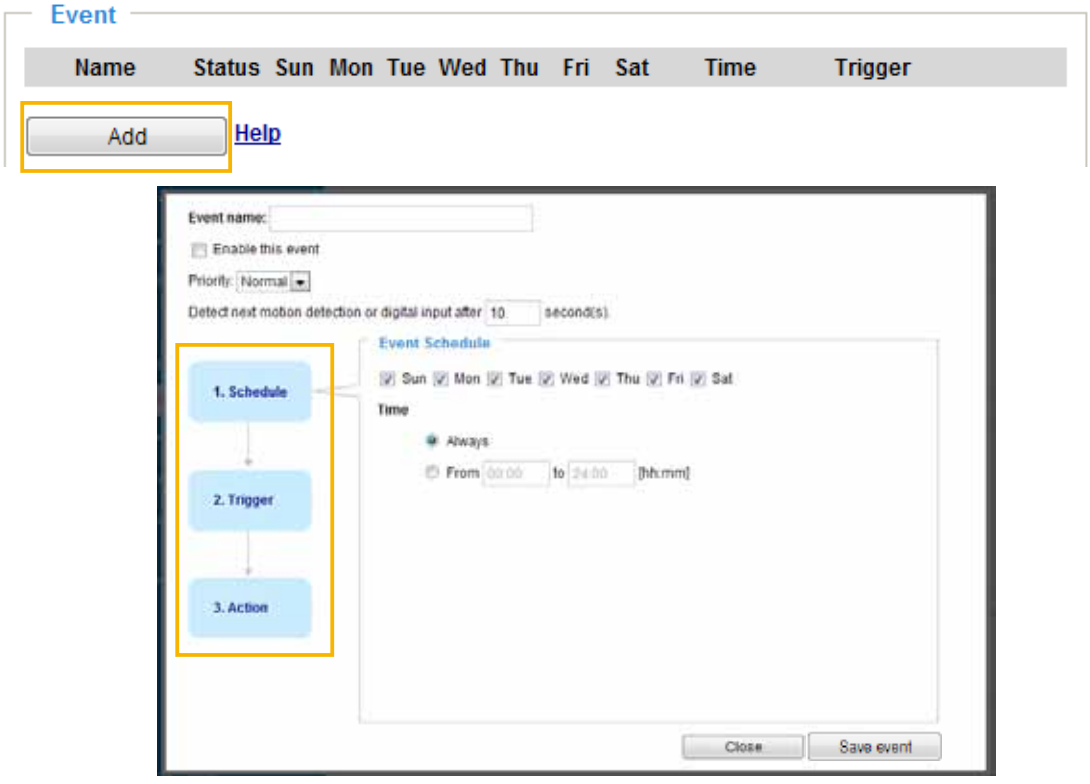
Event > Event settings

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



Event

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window. Here you can arrange three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.



■ Event name: Enter a name for the event setting.

■ Enable this event: Select this option to enable the event setting.

■ Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

■ Detect next motion detection or digital input after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected. This can prevent event-related actions to be too frequently performed.

1. Schedule

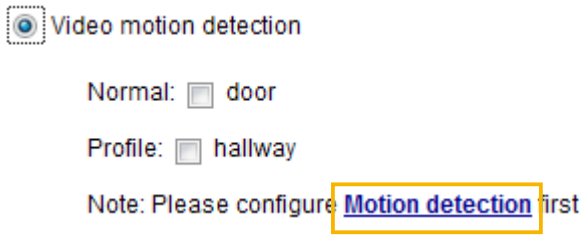
Specify the period of time during which the event trigger will take place. Please select the days of the week and the time in a day (in a 24-hr time format) for the event triggering schedule.

2. Trigger

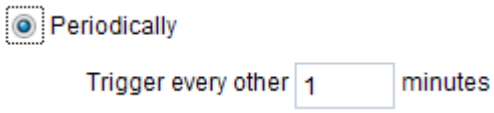
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown on next page. Select the item to display the detailed configuration options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 112 for details.



■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



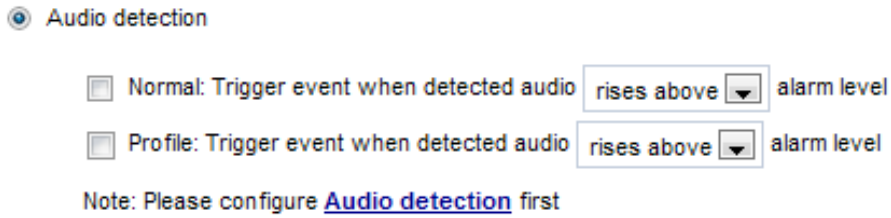
■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Audio detection

A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera's view.



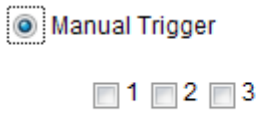
Once you have a preset audio alarm level, you can define the triggering condition either as an audio input rises above or falls below the alarm level.

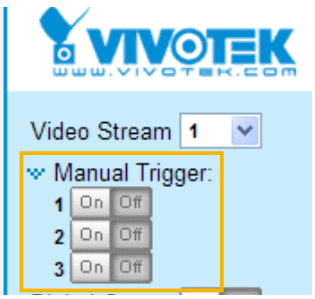
■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 115 for detailed information.

■ Manual Trigger

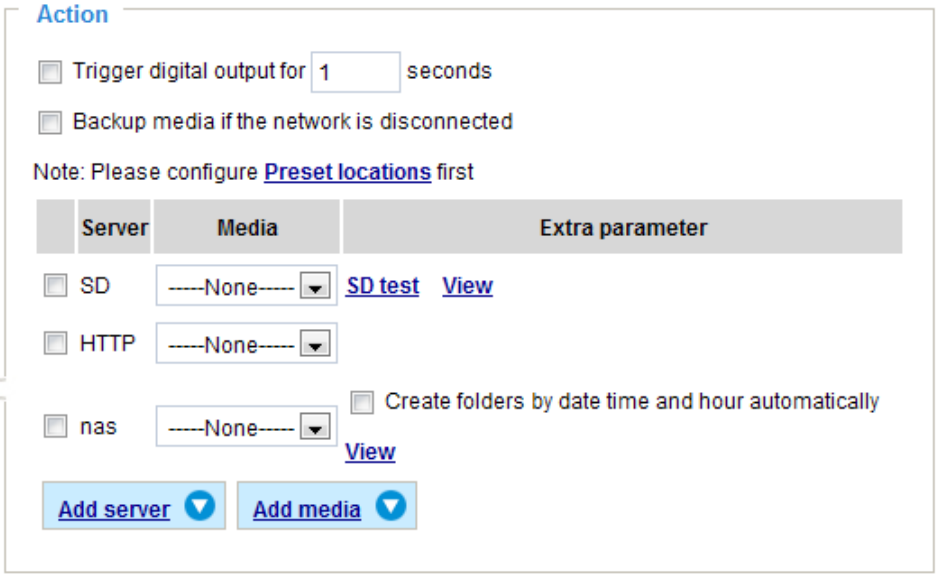
This option allows users to enable event triggers manually by clicking the on/off button on the homepage. Please configure 1 to 3 associated events before using this function.





3. Action

Define the actions to be performed by the Network Camera when a trigger is activated.



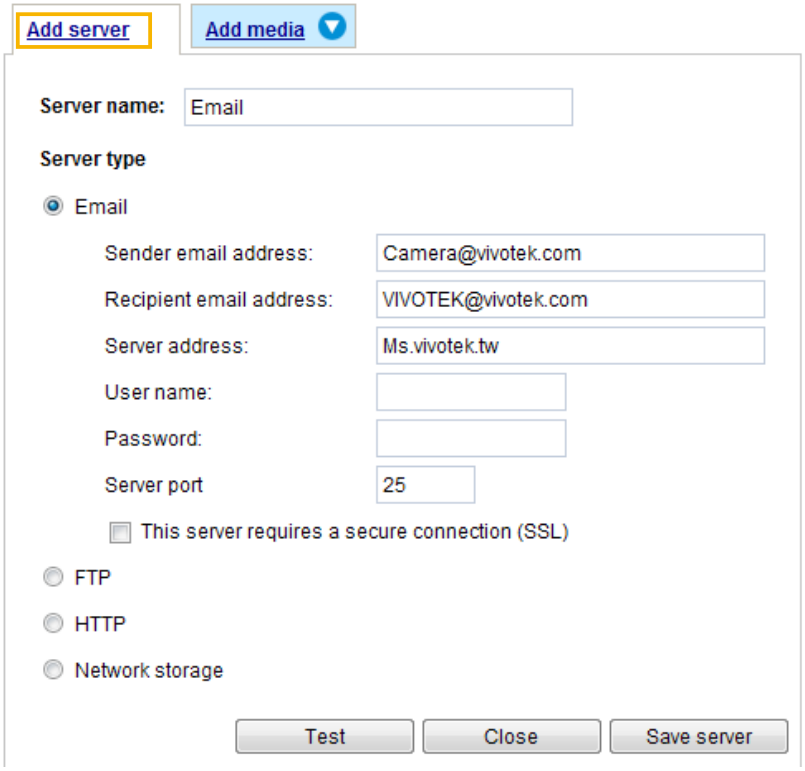
■ Trigger digital output for ☐ seconds
Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Backup media if the network is disconnected
Select this option to backup media file on SD card if the network is disconnected. This function will only be displayed after you set up a networked storage (NAS).

Add server

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. Click **Add server** to open the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.



Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

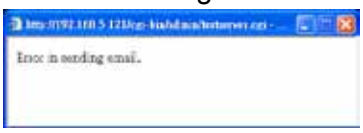
■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

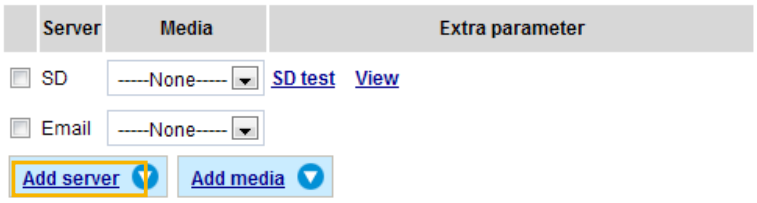
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.



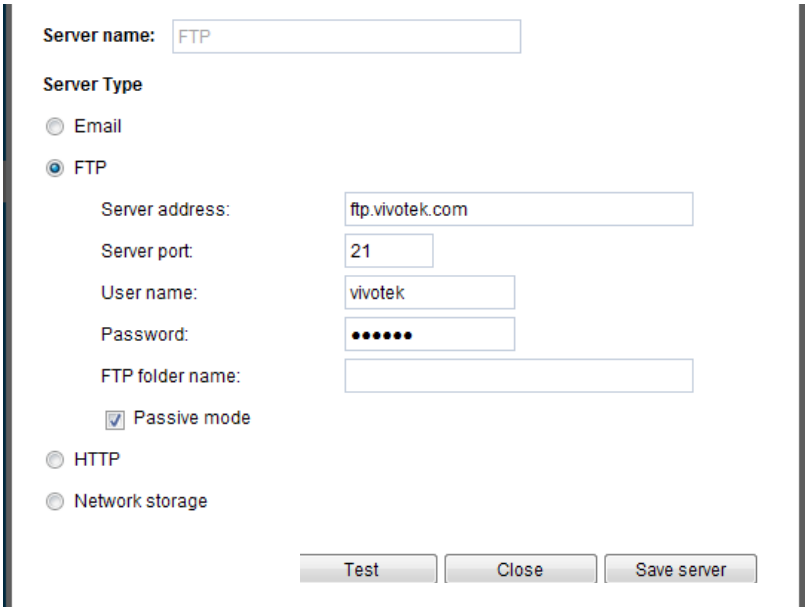
Click **Save server** to enable the settings.

Note that after you set up the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.



Server type - FTP

Select to send the media files to an FTP server when a trigger is activated.



■ Server name: Enter a name for the server setting.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

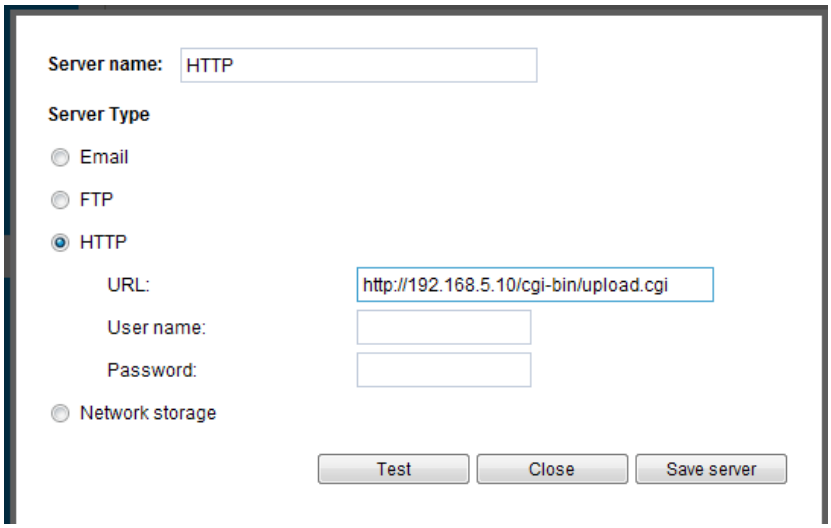
■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will automatically create one on the FTP server.

■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall. The firmware default has the Passive mode checkbox selected.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.

Click **Save server** to enable the settings.

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.



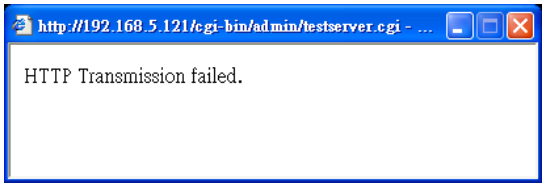
■ Server name: Enter a name for the server setting.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

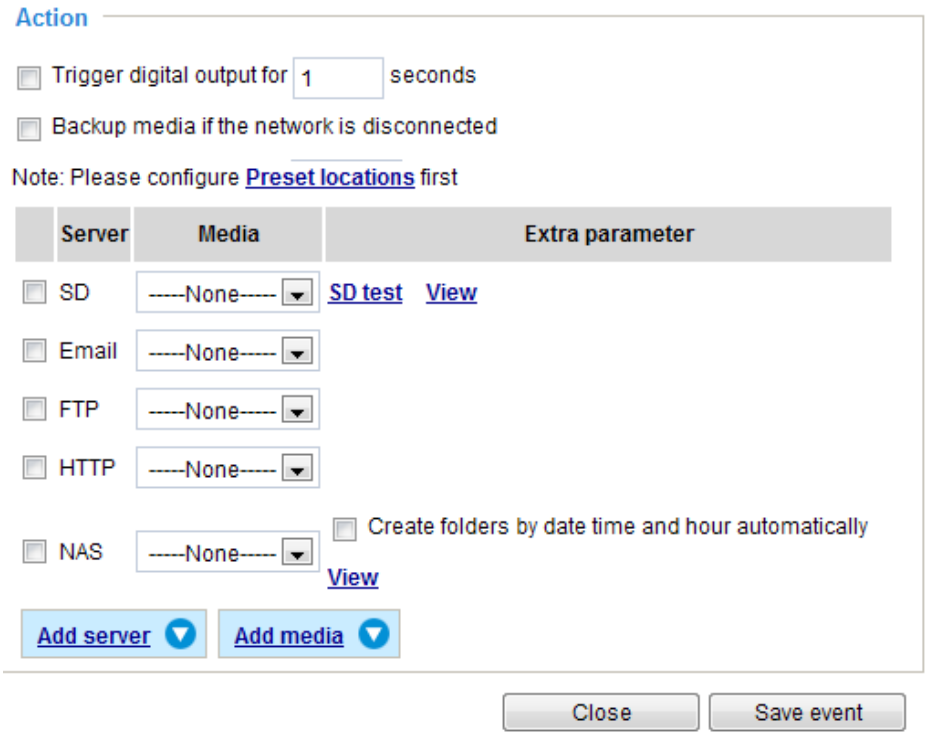
To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



Click **Save server** to enable the settings.

Network storage:
Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 122 for details.

Click **Save server** to enable the settings.

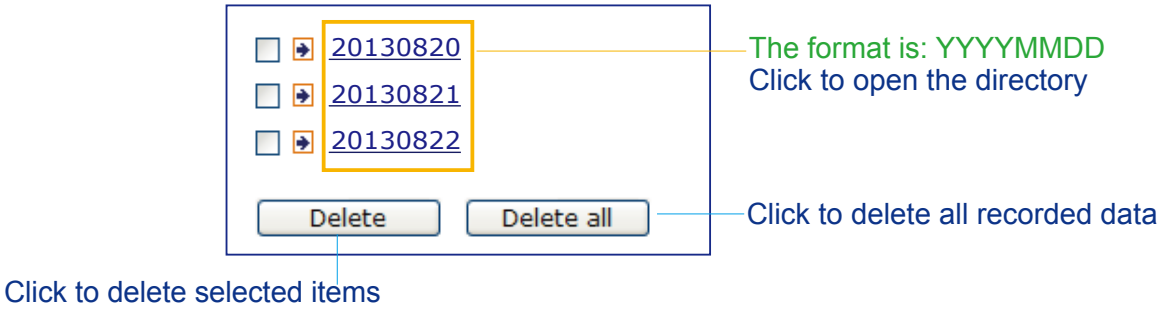


- SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 125 for detailed information.

- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 125. If you click the View button of Network storage, a file directory window will pop up for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.

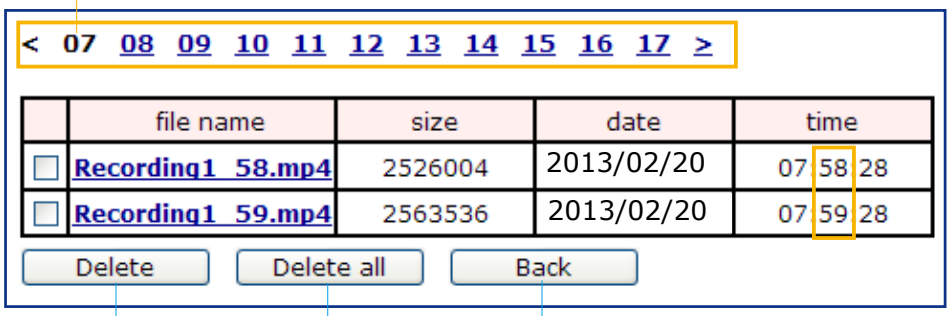
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by the date when video footages are stored onto the networked storage.

The following is an example of a file destination with video clips:



Click **20130220** to open the directory:

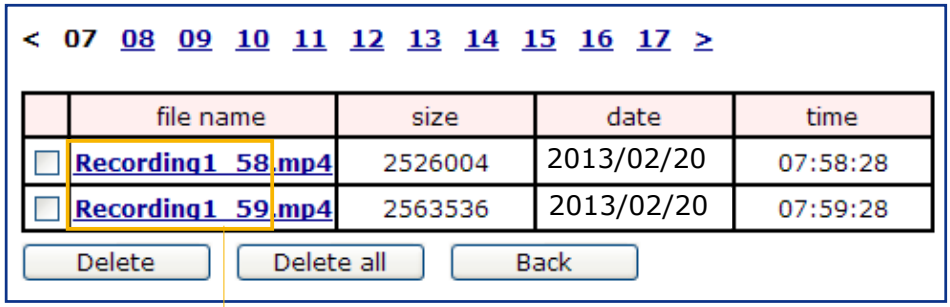
The format is: HH (24r)
Click to open the file list for that hour



Click to delete selected items

Click to delete all recorded data

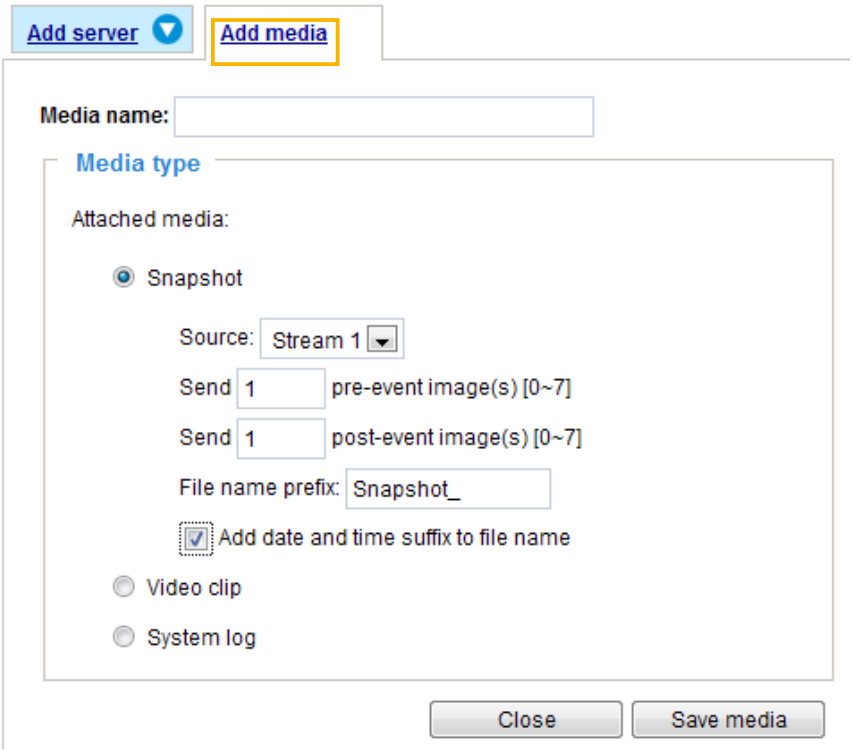
Click to go back to the previous level of the directory



The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Add media page. Please refer to next page for detailed information.

Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.



Media type - Snapshot
Select to send snapshots when a trigger is activated.

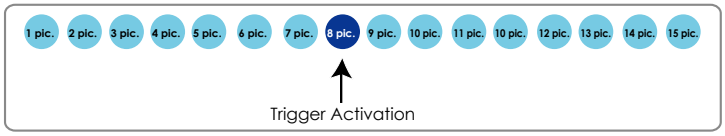
■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from a video stream.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

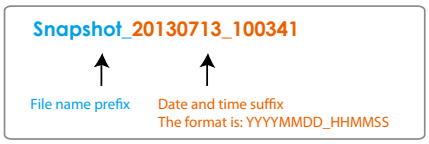
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



■ File name prefix
Enter the text that will be appended to the front of the file name.

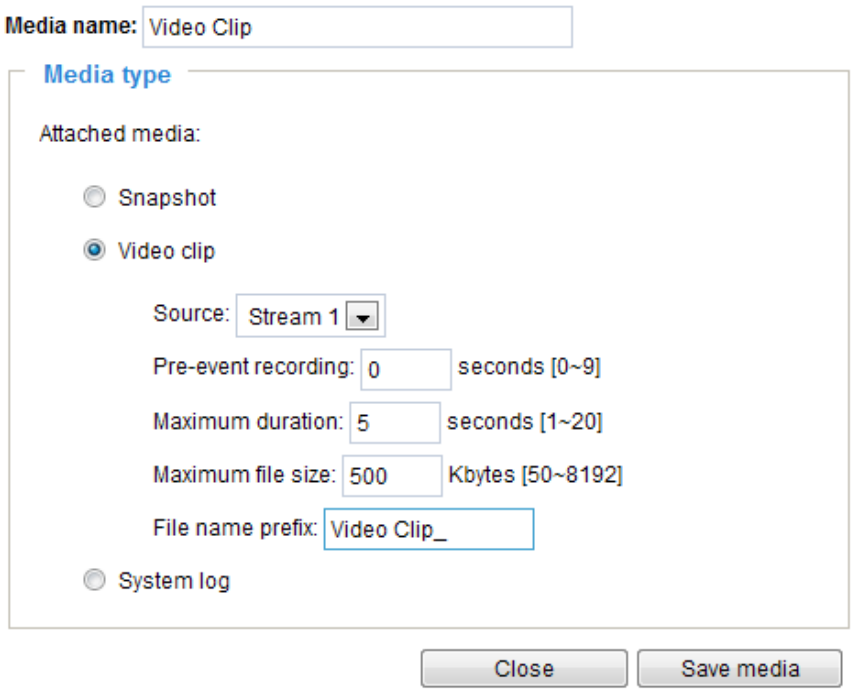
■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:



Click **Save media** to enable the settings.

To note that after you set up the first media server, a new column for media server will automatically show up on the Media list. If you wish to add more other media options, click **Add media**.

Media type - Video clip
Select to send video clips when a trigger is activated.

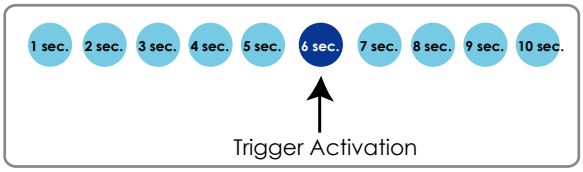


■ Media name: Enter a name for the media setting.

■ Source: Select the source of video clip.

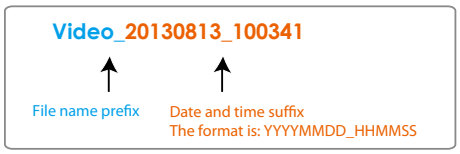
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



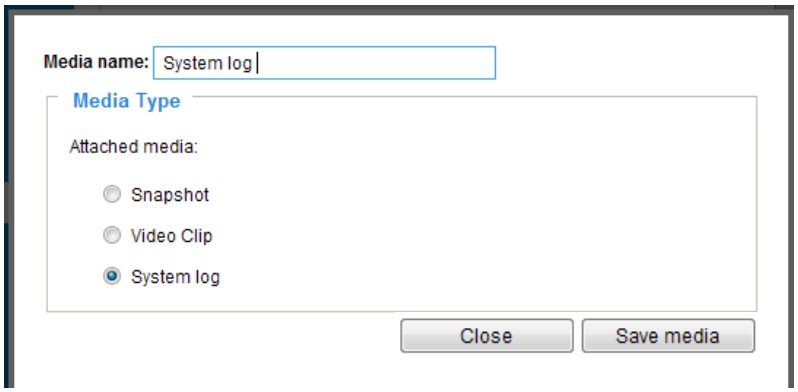
■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

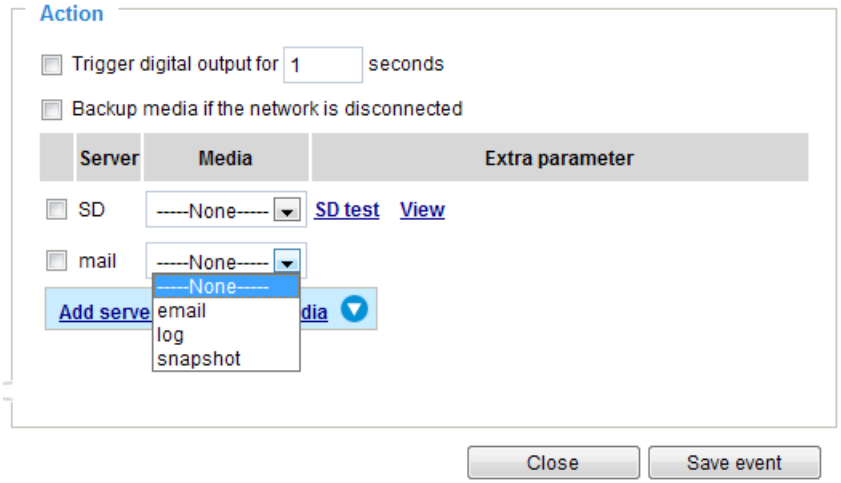


Click **Save media** to enable the settings.

Media type - System log
Select to send a system log when a trigger is activated.



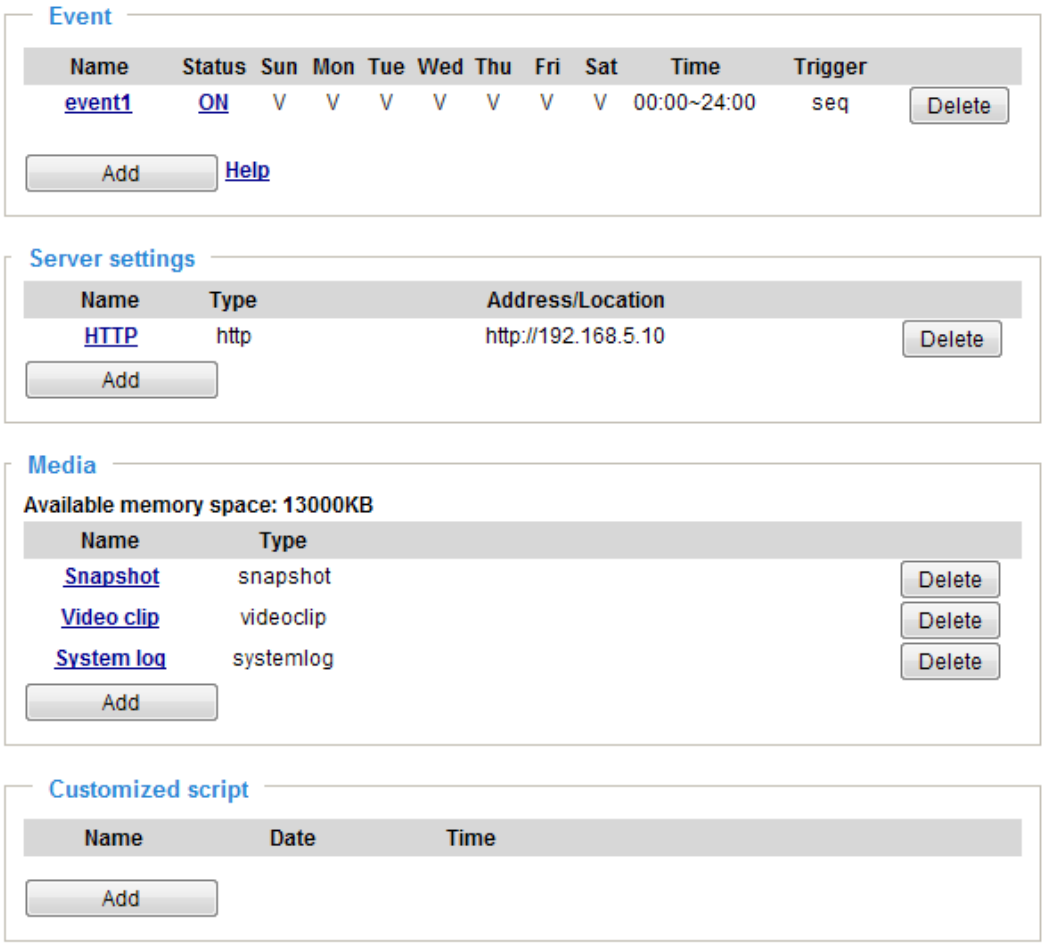
Click **Save media** to enable the settings, then click **Close** to exit the page.



In the Event settings column, the Servers and Medias you configured will be listed; please make sure the Event -> Status is indicated as **ON**, in order to enable the event triggering action.

When completed, click **Save event** to enable the settings and click **Close** to exit Event Settings page. The new Event / Server settings / Media will appear in the event drop-down list on the Event setting page.

Please see the example of the Event setting page below:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

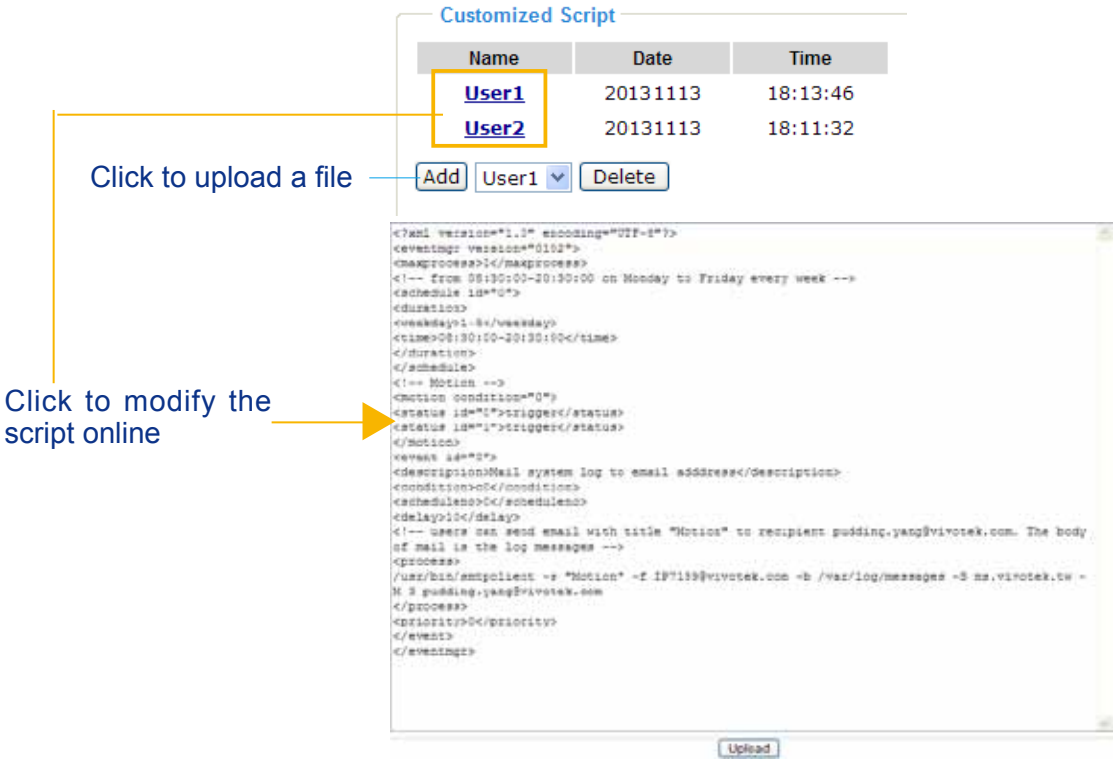
If you want to stop the event trigger, you can click on the **ON** button to turn its status to **OFF** or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that you can only delete a server setting when it is not applied to an existing event setting.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that you can only delete a media setting when it is not applied to an event setting.

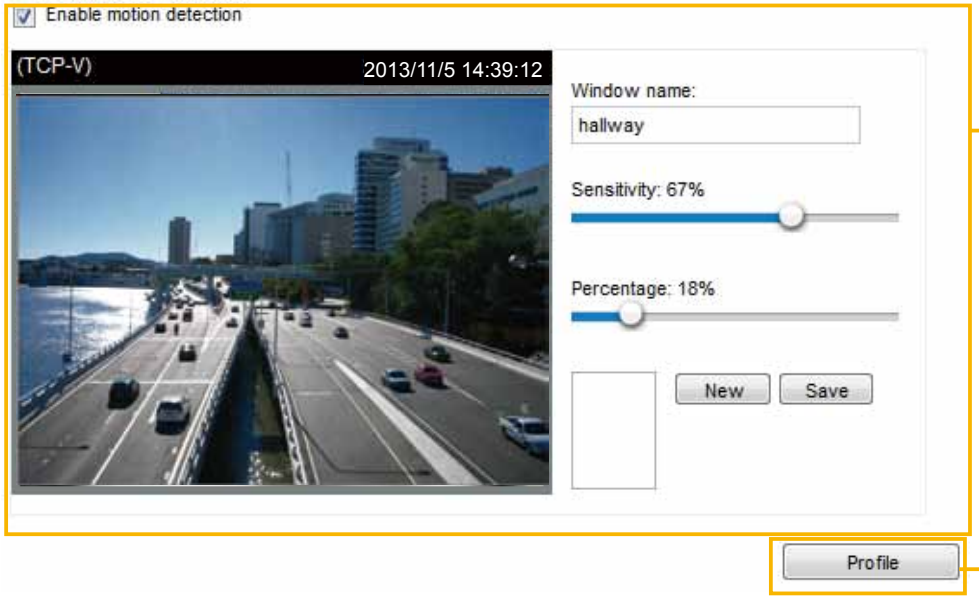
Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK technical support.



Applications > Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



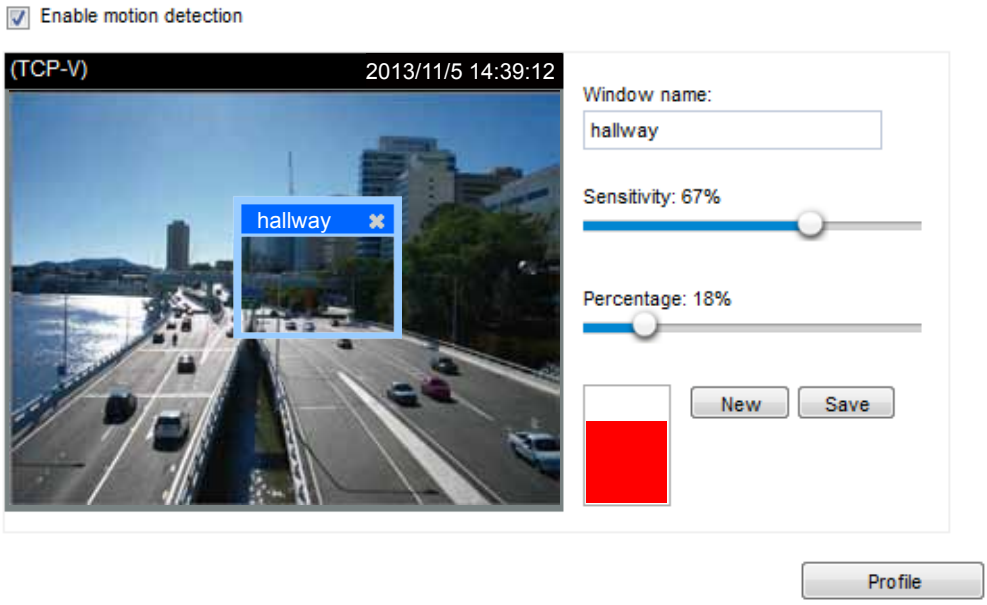
Motion Detection Setting 1: For normal situations

Motion Detection Setting 2: For special situations

Follow the steps below to enable motion detection:

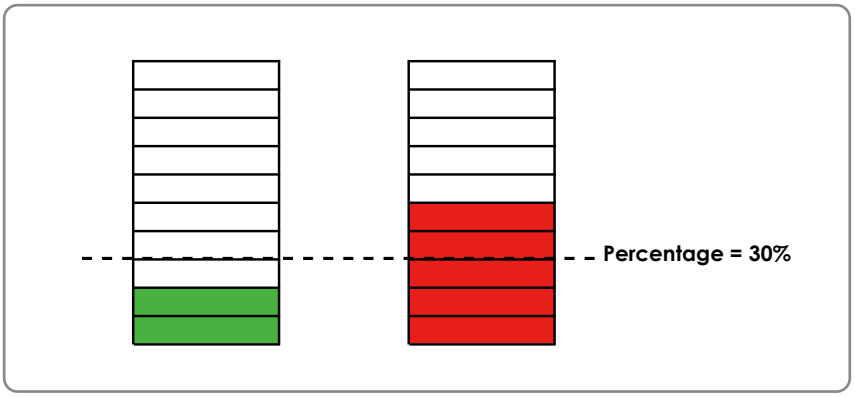
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - To move and resize the window, drag and drop your mouse on the window.
   - To delete a window, click X on the upper right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:

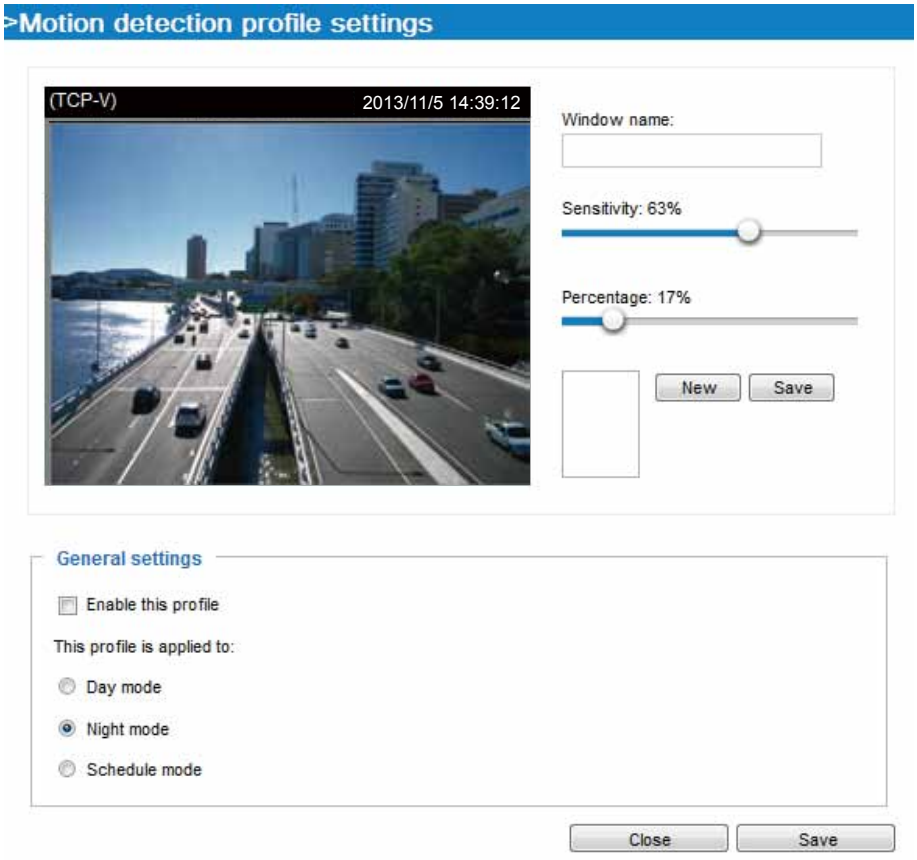


The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Event settings on page 98.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.

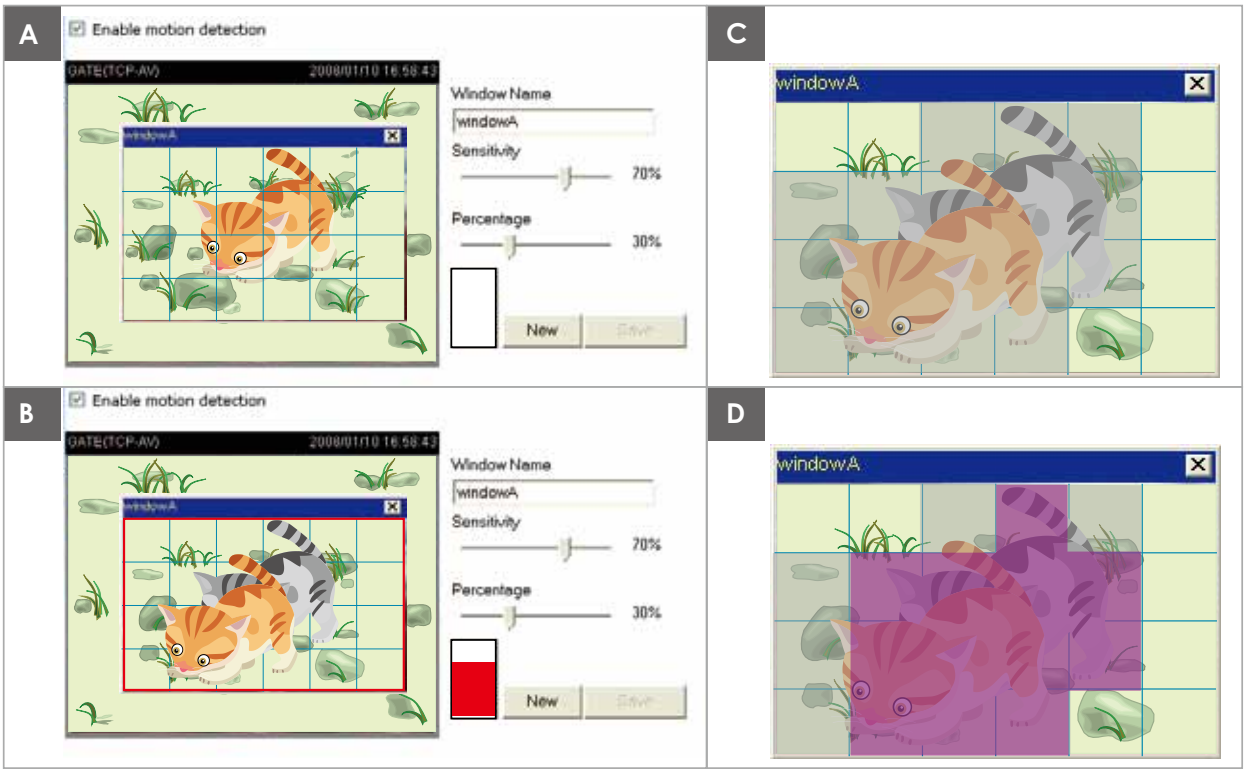


Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 121 for detailed information.

NOTE:

► *How does motion detection work?*

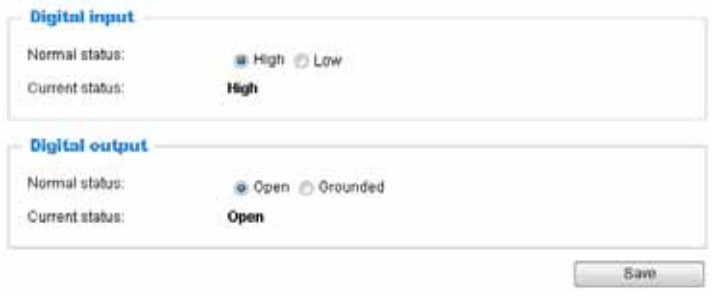


There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Applications > DI and DO



Connect DI or DO devices to the camera's terminal block, the camera will automatically detect the current connection state as pulled-high or pulled-low. You may then define the triggering condition.

Digital input: Select High or Low to define the "active state" for the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define the "active state" for the digital output. The Network Camera will show whether the trigger is activated or not.

Applications > Tampering detection

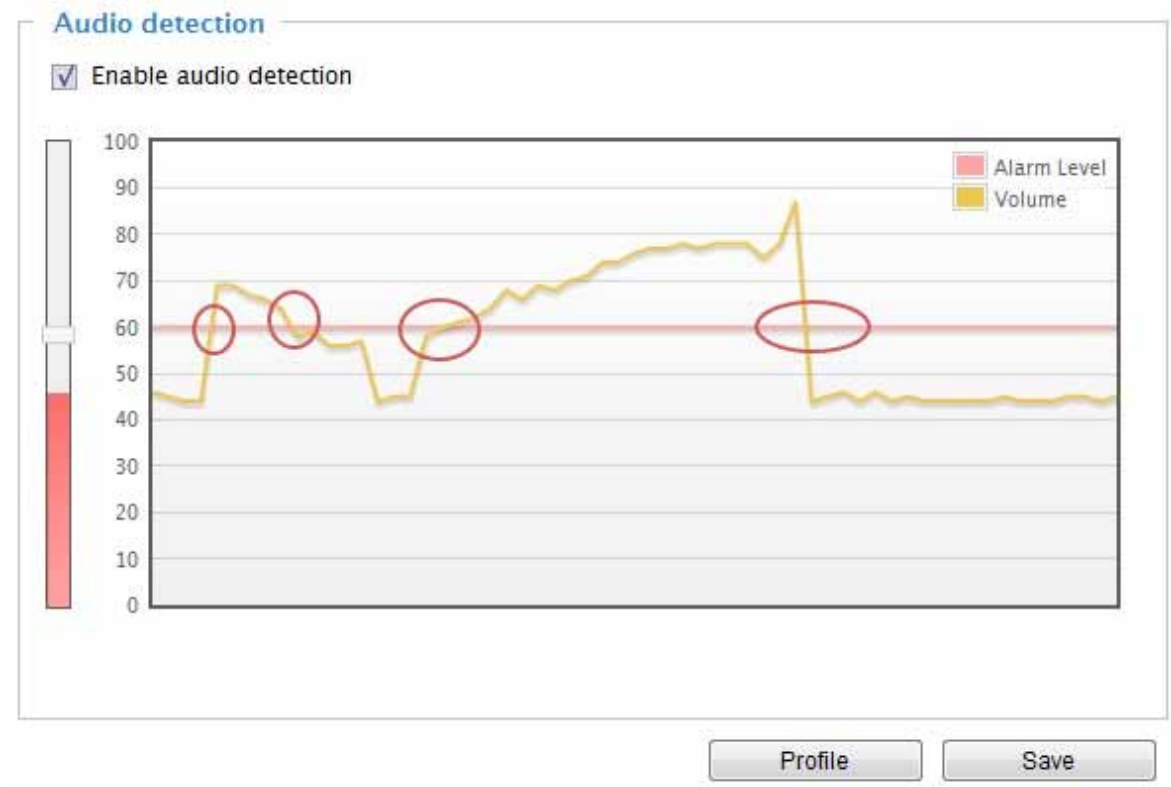
This section explains how to set up camera tamper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

Please follow the steps below to set up the camera tamper detection function:

1. Check **Enable camera tampering detection**.
2. The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Event > Event settings > Trigger.** Please refer to page 121 for detailed information.

Applications > Audio detection

Audio detection, along with video motion detection, is applicable in the following scenarios:
1. Detection of activities not covered by camera view, e.g., a loud input by gun shots or breaking a door/window.
2. A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
3. A PTZ camera can be directed to turn to a preset point by the occurrence of audio events.
4. Dark environments where video motion detection may not function well.



The red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

How to configure Audio detection:
1. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.
3. Select the “Enable audio detection“ checkbox and click Save to enable the feature.

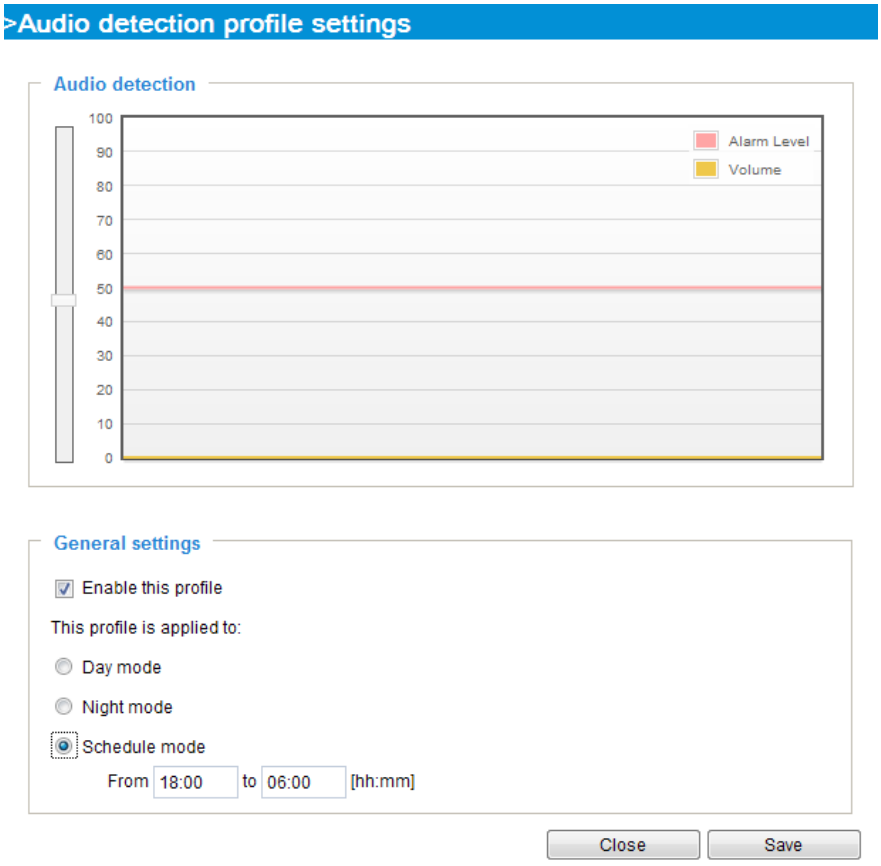
NOTE:

1. Note that the volume numbers (0~100) on the side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.

2. To configure this feature, you must not mute the audio in **Configuration > Media > Audio***. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.*

You can use the **Profile** window to configure a different Audio detection setting. For example, a place can be noisy in the day time and become very quiet in the night.

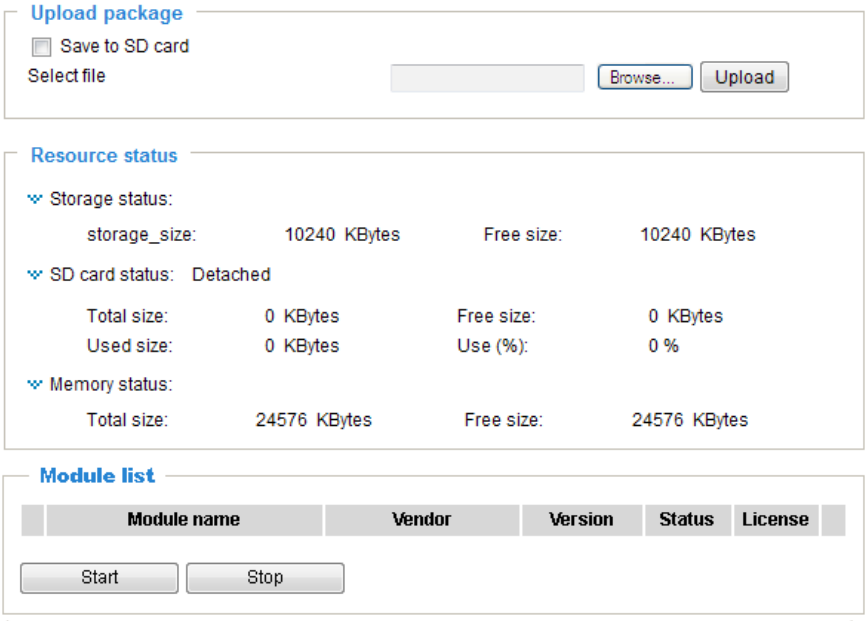
1. Click on the **Enable this profile** checkbox. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Use a mouse click to drag the **Alarm level** tab to a preferred location on the slide bar.
3. Select the **Day**, **Night**, or **Schedule** mode check circles. You may also manually configure a period of time during which this profile will take effect.
4. Click **Save** and then click **Close** to complete your configuration.



IMPORTANT:

- If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.
- To configure and enable this feature, you **must not** configure video stream #1 into **Motion JPEG**. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station **along with stream #1**.
- Refer to page 62 for Audio settings, and page 58 for video streaming settings.

Applications > VADP (VIVOTEK Application Development Platform)



Users can store and execute VIVOTEK's or 3rd-party software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting, or as an agent for edge recording, etc.

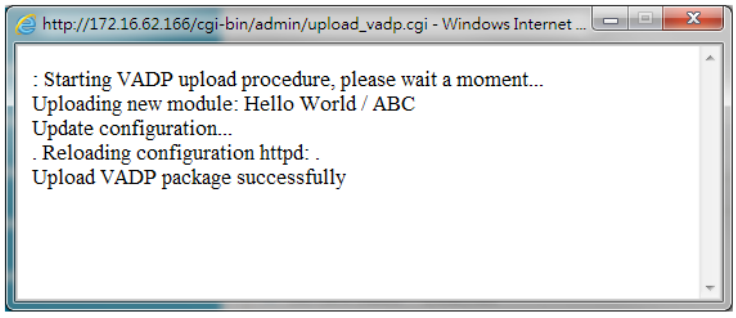
- Once the software package is successfully uploaded, the module configuration (vadp.xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined VADP requirements. Please contact technical support or the vendor of your 3rd-party module for the parameters contained within.

- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.

- Note that for some cameras the flash is too small to hold VADP packages. These cameras will have its "Save to SD card" checkbox selected and grayed-out for all time.

- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

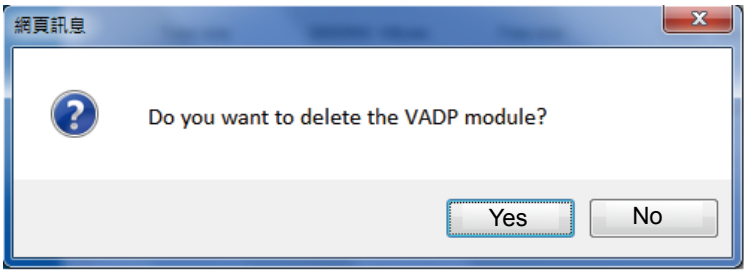
To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:


http://172.16.62.166/cgi-bin/admin/upload_vadp.cgi - Windows Internet ...
: Starting VADP upload procedure, please wait a moment...
Uploading new module: Hello World / ABC
Update configuration...
. Reloading configuration httpd: .
Upload VADP package successfully

To start a module, select the checkcircle in front, and click the **Start** button.

If you should need to remove a module, select the checkcircle in front and then click the **Stop** button. By then the module status will become **OFF**, and the **X** button will appear at the end of the row. Click on the **X** button to remove an existing module.

When prompted by a confirm message, Click **Yes** to proceed.

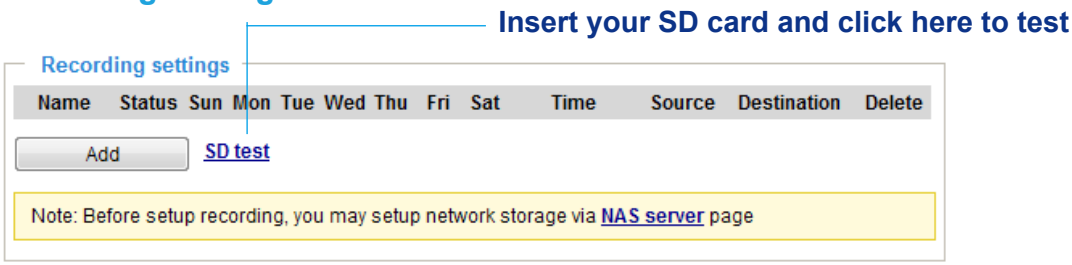


Note that the actual memory consumed while operating the module will be indicated on the **Memory status** field. This helps determine whether a running module has consumed too much of system resources.

Recording > Recording settings

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

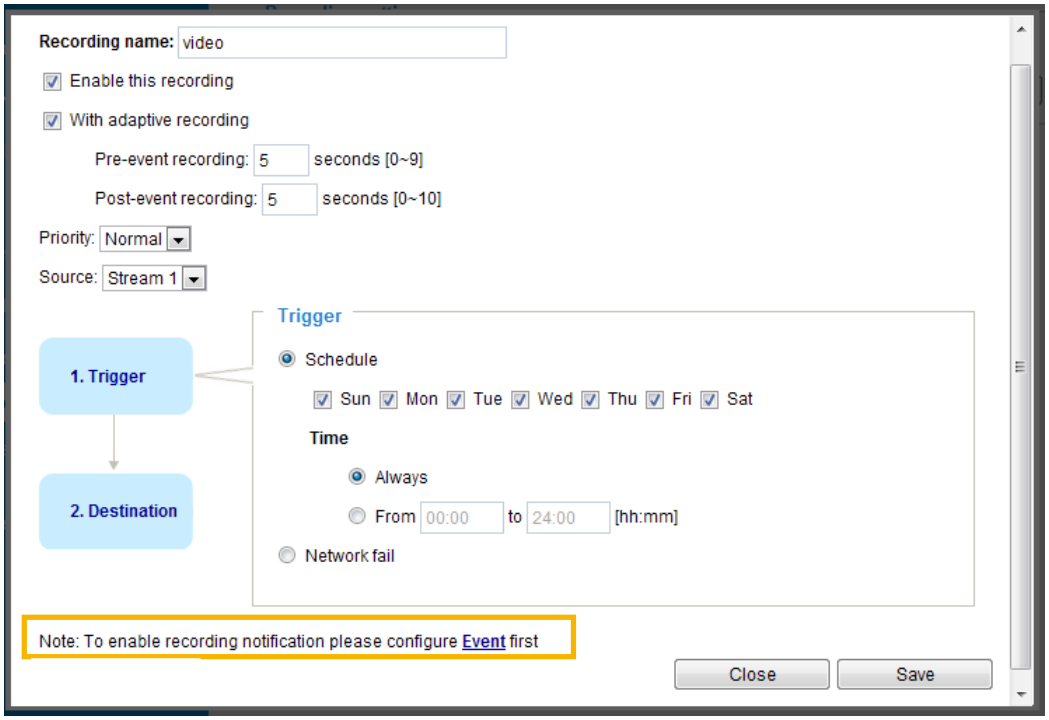

Insert your SD card and click here to test
Recording settings
Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete
Add
SD test
Note: Before setup recording, you may setup network storage via NAS server page

NOTE:

► *Please remember to format your SD card when using it for the first time. Please refer to page 125 for detailed information.*

Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

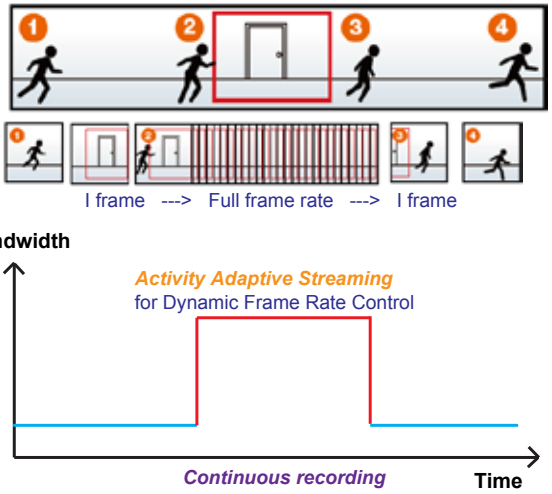


■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:
Select this option will activate the frame rate control according to alarm trigger.
The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've set on Video quality page. Please refer to page 59 for more information.

If you enable adaptive recording and enable time-shift cache stream on Camera A, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidths and storage space.



NOTE:

► *To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.*

► *When there is no alarm trigger:*
- JPEG mode: record 1 frame per second.
- H.264 mode: record I frame only.
- MPEG-4 mode: record the I frame only.

► *When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.*

The alarm trigger includes: motion detection and DI detection. Please refer to Event Settings on page 98.

■ Pre-event recording and post-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

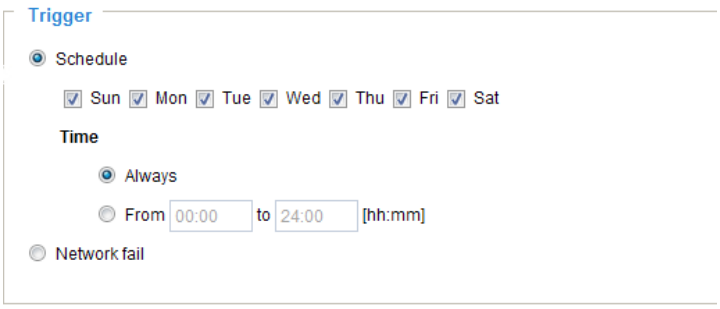
■ Source: Select a stream for the recording source.

NOTE:

► *To enable recording notification please configure **Event settings** first . Please refer to page 98.*

Please follow the steps below to set up the recording.

1. Trigger
Select a trigger source.



■ Schedule: The server will start to record files on the local storage or network storage (NAS).

■ Network fail: Since network fail, the server will start to record files on the local storage (SD card).

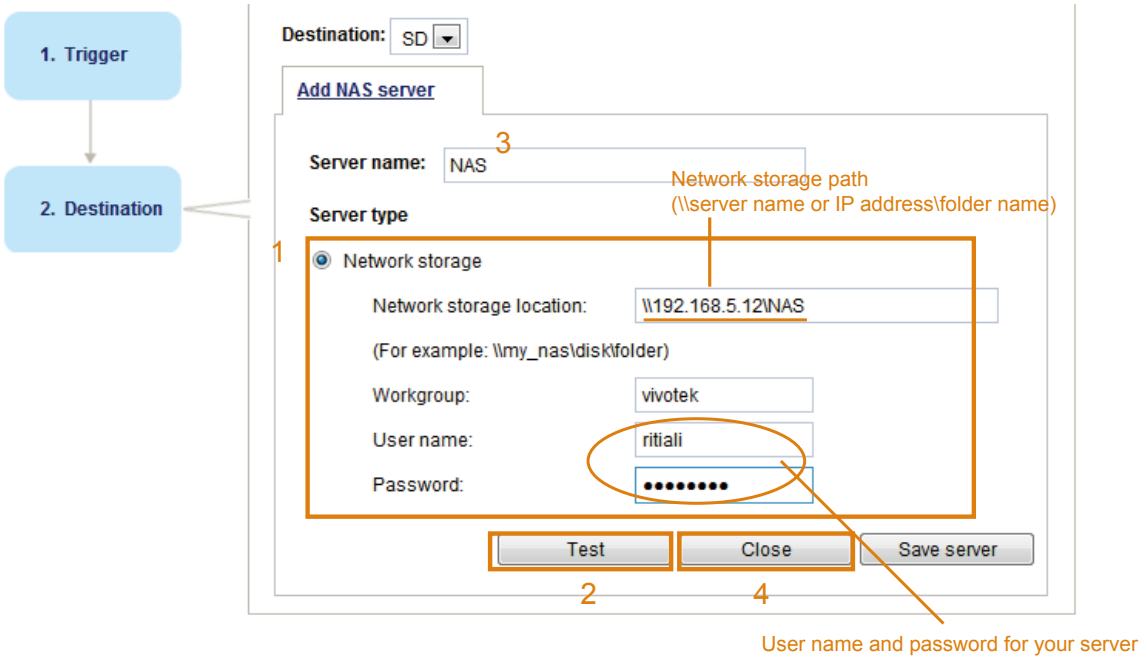
2. Destination

You can select the SD card or network storage (NAS) for the recorded video files.

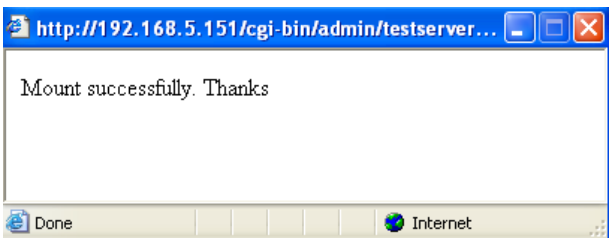
NAS server

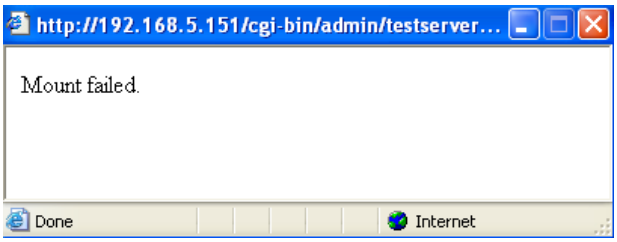
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for your server.
   For example:

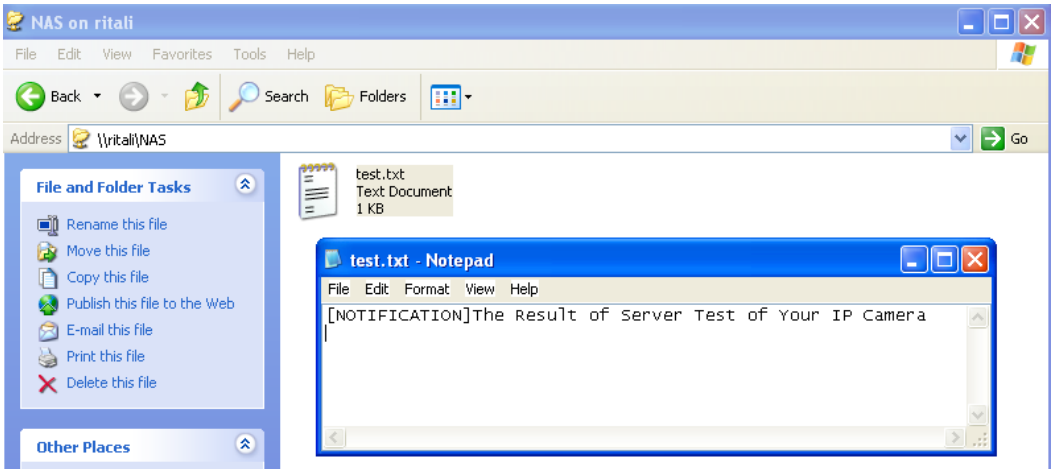


2. Click **Test** to check the setting. The result will be shown in the pop-up window.

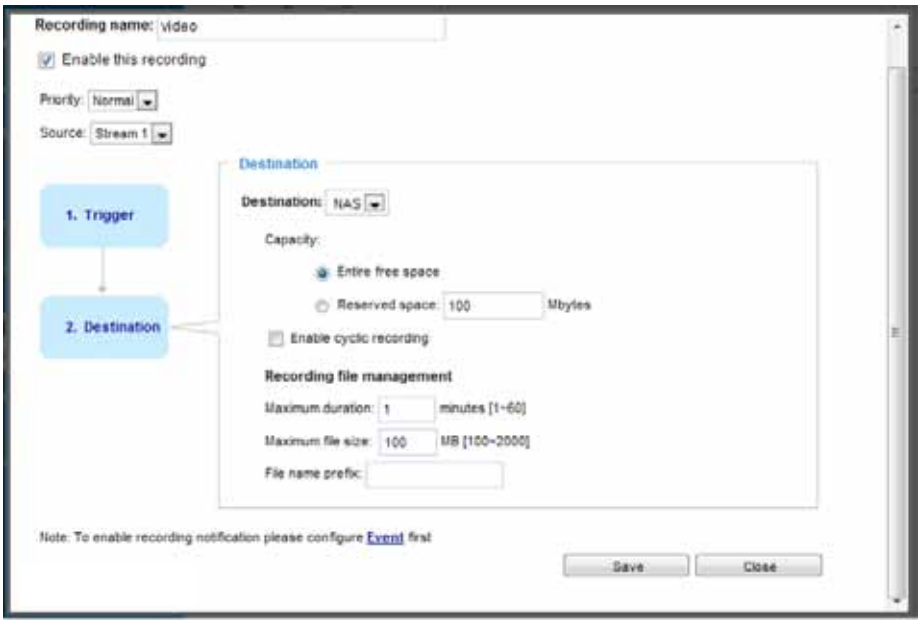




If successful, you will receive a test.txt file on the network storage server.



3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.



■ Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

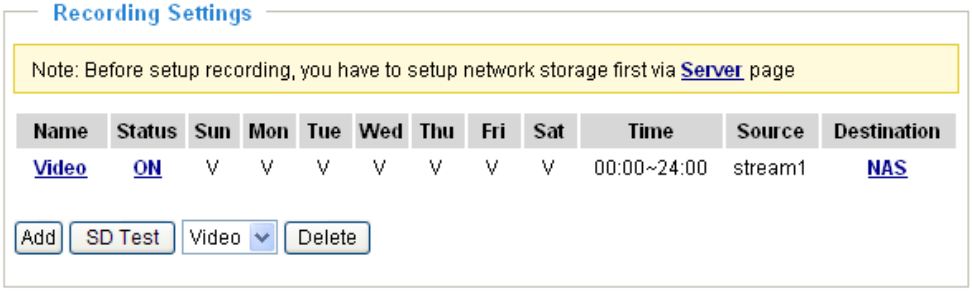
■ File name prefix: Enter the text that will be appended to the front of the file name.

■ Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MBytes.

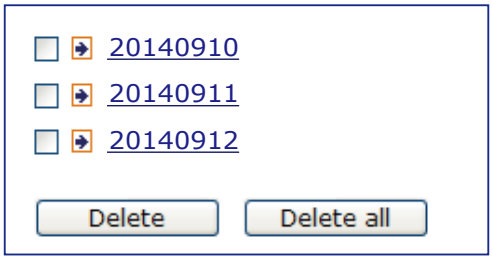
f you want to enable recording notification, please click ***Event*** to configure event triggering settings. Please refer to **Event > Event settings** on page 98 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.



- Click **Video (Name)**: Opens the Recording Settings page to modify.
- Click **ON (Status)**: The Status will become **OFF** and stop recording.
- Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 122 for details.

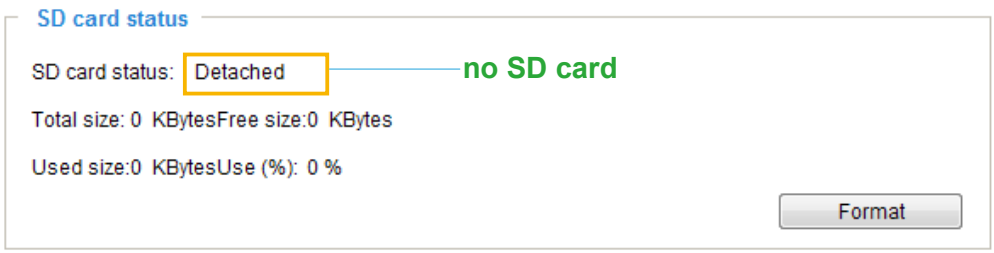


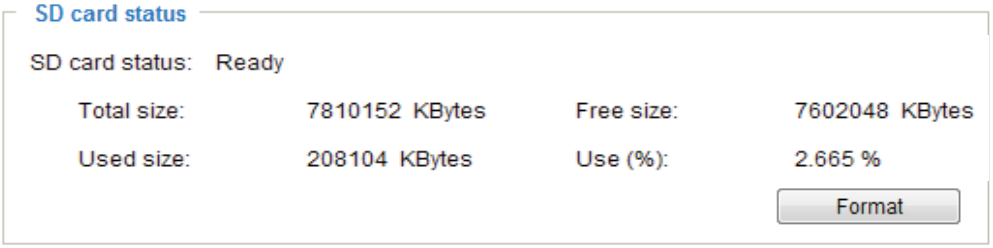
Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

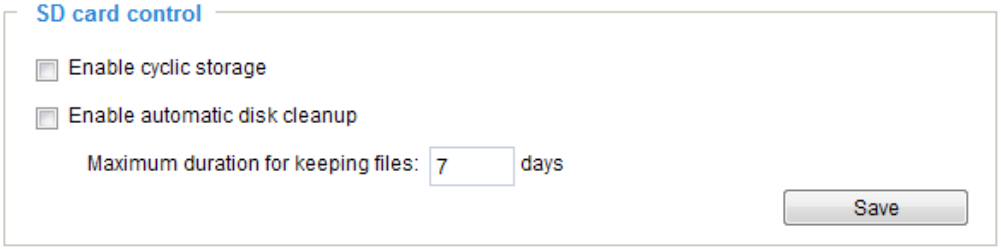
SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.





SD card control



- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

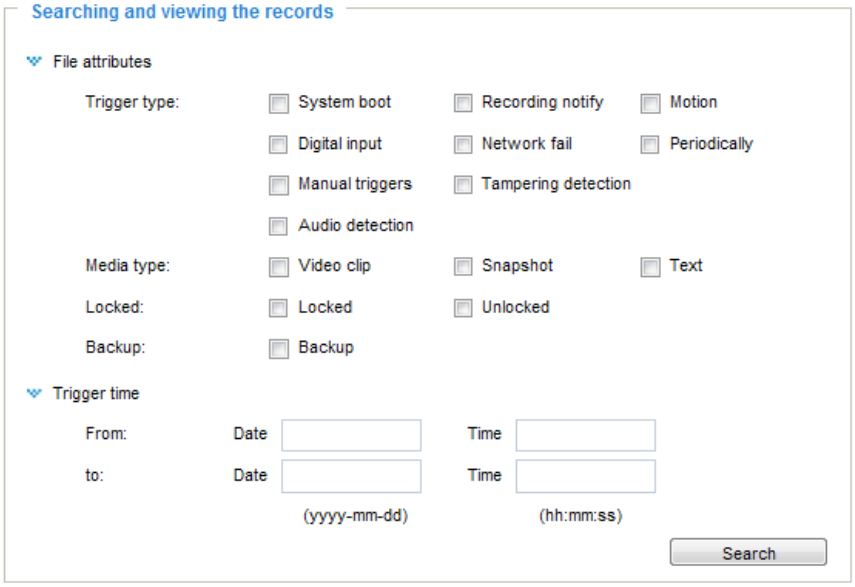
Click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** column.

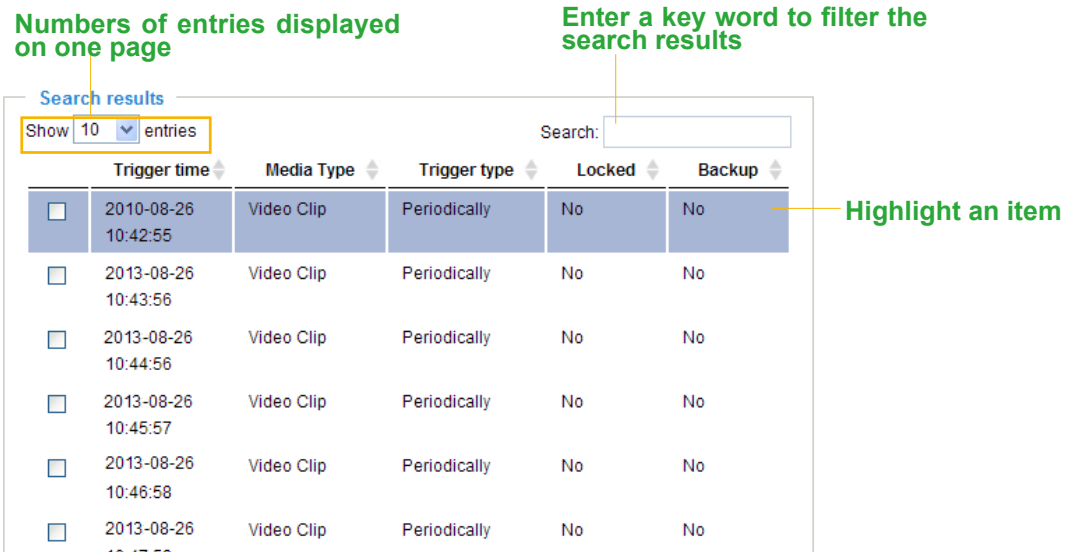


■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⇕ to sort the search results in either direction.

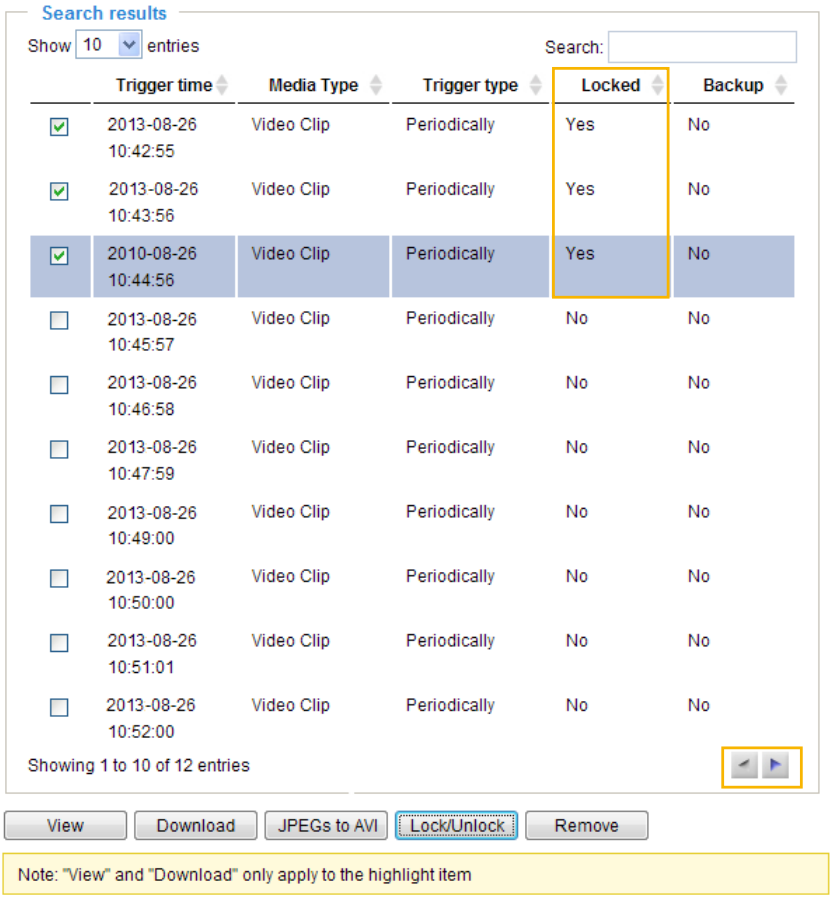


■ View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file. For example:

■ Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

■ JPEGs to AVI: This functions only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

■ Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections. For example:


Search results
Show 10 entries
Search:
Trigger time
Media Type
Trigger type
Locked
Backup
2013-08-26 10:42:55 Video Clip Periodically Yes No
2013-08-26 10:43:56 Video Clip Periodically Yes No
2010-08-26 10:44:56 Video Clip Periodically Yes No
2013-08-26 10:45:57 Video Clip Periodically No No
2013-08-26 10:46:58 Video Clip Periodically No No
2013-08-26 10:47:59 Video Clip Periodically No No
2013-08-26 10:49:00 Video Clip Periodically No No
2013-08-26 10:50:00 Video Clip Periodically No No
2013-08-26 10:51:01 Video Clip Periodically No No
2013-08-26 10:52:00 Video Clip Periodically No No
Showing 1 to 10 of 12 entries
Click to switch pages
View
Download
JPEGs to AVI
Lock/Unlock
Remove
Note: "View" and "Download" only apply to the highlight item

■ Remove: Select the desired search results, then click this button to delete the files.

Appendix

URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

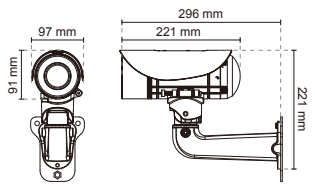
```
http://mywebserver/cgi-bin/viewer/video.jpg
```

Technical Specifications

Technical Specifications

Model	IP8355H/55EH
System Information	
CPU	Multimedia SoC (System-on-Chip)
Flash	256 MB
RAM	384 MB
Camera Features	
Image Sensor	1/3" Progressive CMOS
Maximum Resolution	1280x1024 (1.3MP)
Lens Type	Vari-focal, Remote Focus
Focal Length	f = 3 ~ 9 mm
Aperture	F1.2 ~ F2.3
Auto-iris	P-iris
Field of View	34° ~ 80° (Horizontal) 27° ~ 62° (Vertical) 44° ~ 101° (Diagonal)
Shutter Time	1/5 sec. to 1/10,000 sec.
WDR Technology	WDR Pro II
Day/Night	Removable IR-cut filter for day & night function Smart IR Technology to avoid overexposure
Minimum Illumination	0.04 Lux @ F1.2 (Color) 0.001 Lux @ F1.2 (B/W)
Pan/tilt/zoom Functionalities	ePTZ: 48x digital zoom (4x on IE plug-in,12x built in)
IR Illuminators	Built-in IR illuminators, effective up to 30 meters IR LED*4, with Smart IR Technology
On-board Storage	SD/SDHC/SDXC card slot
Video	
Compression	H.264, MJPEG
Maximum Frame Rate	30 fps @ 1280x1024 60 fps @ 1280x1024 (one-stream mode only) In both compression modes
Maximum Streams	2 simultaneous streams
S/N Ratio	64dB
Dynamic Range	140dB
Video Streaming	Adjustable resolution, quality and bitrate
Image Settings	Time stamp, text overlay, flip & mirror configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks, scheduled profile settings, 3D Noise Reduction, EIS, Video Rotation
Audio	
Audio Capability	Two-way audio (full duplex)
Compression	AAC, G.711, G.726
Interface	External microphone input Audio output
Network	
Users	Live viewing for up to 10 clients
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X, UDP, ICMP
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)
ONVIF	Supported, specification available at www.onvif.org
Intelligent Video	
Video Motion Detection	Triple-window video motion detection
Alarm and Event	
Alarm Triggers	Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notification, camera tampering detection
Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server
General	
Smart Focus System	Remote focus
Connectors	RJ-45 for Network/PoE connection Audio input/output AV output AC 24V power input DC 12V power input Digital input*1 Digital output*1
LED Indicator	System power and status indicator
Power Input	DC12V/AC24V IEEE 802.3af PoE
Power Consumption	IP8355H: DC Max. 11 W AC Max. 24.4 W PoE Max. 11 W IP8355EH: DC Max. 30 W (Heater on), 8 W (Heater off) AC Max. 30 W (Heater on), 8.8 W (Heater off) PoE Max. 11 W (Heater off)
Dimensions	Ø: 91 mm x 221 mm
Weight	Body only Net: 1,314g (IP8355EH), 1,270g (IP8355H) With stand and sunshield Net: 1,911g (IP8355EH), 1,867g (IP8355H)
Casing	Weather-proof IP67-rated housing
Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick, UL
Operating Temperature	IP8355H: Starting Temperature: -10°C ~ 50°C (14°F ~ 122°F) Working Temperature: -20°C ~ 50°C (-4°F ~ 122°F) IP8355EH: Starting Temperature: -40°C ~ 50°C (-40°F ~ 122°F) (PoE: -10°C ~ 50°C) Working Temperature: -50°C ~ 50°C (-58°F ~ 122°F)
Warranty	24 months
System Requirements	
Operating System	Microsoft Windows 8/7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~10 (streaming only) Internet Explorer 7/8/9/10
Other Players	VLC: 1.1.11 or above Quicktime: 7 or above
Included Accessories	
CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Others	Quick installation guide, warranty card, sun shield, wall mount bracket, waterproof RJ45 Ethernet enclosure, alignment sticker, desiccant bag, waterproof connector

Dimensions



Compatible Accessories

Mounting Kits

AM-311
Pole Mount Adaptor

AM-411
Corner Mount Adaptor

PoE Kits

POE-IJ-1748NDN
PoE injector, 802.3af compliant

All specifications are subject to change without notice. Copyright © VIVOTEK INC. All rights reserved.

Distributed by:

Ver 1.3

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho,
New Taipei City, 235, Taiwan, R.O.C.
T: +886-2-82455282 F: +886-2-82455532
E: sales@vivotek.com

VIVOTEK USA
2050 Ringwood Avenue,
San Jose, CA 95131
T: 408-773-8686 F: 408-773-8298
E: salesusa@vivotek.com

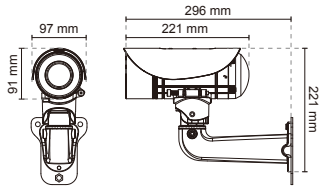
VIVOTEK Europe
Randstad 22-133, 1316BW Almere,
The Netherlands
E: saleseurope@vivotek.com

Technical Specifications

Model	IP8365H/65EH
System Information	
CPU	Multimedia SoC (System-on-Chip)
Flash	256 MB
RAM	384 MB
Camera Features	
Image Sensor	1/2.8" Progressive CMOS
Maximum Resolution	1920x1080 (2MP)
Lens Type	Vari-focal, Remote Focus
Focal Length	f = 3 ~ 9 mm
Aperture	F1.2 ~ F2.3
Auto-iris	P-Iris
Field of View	39° ~ 89° (Horizontal) 22° ~ 49° (Vertical) 44° ~ 103° (Diagonal)
Shutter Time	1/5 sec. to 1/10,000 sec.
WDR Technology	WDR Pro
Day/Night	Removable IR-cut filter for day & night function Smart IR Technology to avoid overexposure
Minimum Illumination	0.11 Lux @ F1.2 (Color) 0.001 Lux @ F1.2 (B/W)
Pan/tilt/zoom Functionalities	ePTZ: 48x digital zoom (4x on IE plug-in,12x built in)
IR Illuminators	Built-in IR illuminators, effective up to 30 meters IR LED*4, with Smart IR Technology
On-board Storage	SD/SDHC/SDXC card slot
Video	
Compression	H.264, MJPEG
Maximum Frame Rate	30 fps @ 1920x1080 60 fps @ 1920x1080 (one-stream mode only) In both compression modes
Maximum Streams	2 simultaneous streams
S/N Ratio	62dB
Dynamic Range	100dB
Video Streaming	Adjustable resolution, quality and bitrate
Image Settings	Time stamp, text overlay, flip & mirror configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks, scheduled profile settings, 3D Noise Reduction, EIS, Video Rotation
Audio	
Audio Capability	Two-way audio (full duplex)
Compression	AAC, G.711, G.726
Interface	External microphone input Audio output
Network	
Users	Live viewing for up to 10 clients
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X, UDP, ICMP
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)
ONVIF	Supported, specification available at www.onvif.org
Intelligent Video	
Video Motion Detection	Triple-window video motion detection

Alarm and Event	
Alarm Triggers	Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notification, camera tampering detection
Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server
General	
Smart Focus System	Remote focus
Connectors	RJ-45 for Network/PoE connection Audio input/output AV output AC 24V power input DC 12V power input Digital input*1 Digital output*1
LED Indicator	System power and status indicator
Power Input	DC12V/AC24V IEEE 802.3af PoE
Power Consumption	IP8365H: DC Max. 11 W AC Max. 24.4 W PoE Max. 11 W IP8365EH: DC Max. 30 W (Heater on), 8 W (Heater off) AC Max. 30 W (Heater on), 8.8 W (Heater off) PoE Max. 11 W (Heater off)
Dimensions	Ø: 91mm x 221mm
Weight	Body only Net: 1,314g (IP8365EH), 1,270g (IP8365H) With stand and sunshield Net: 1,911g (IP8365EH), 1,867g (IP8365H)
Casing	Weather-proof IP67-rated housing
Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick, UL
Operating Temperature	IP8365H: Starting Temperature: -10°C ~ 50°C (14°F ~ 122°F) Working Temperature: -20°C ~ 50°C (-4°F ~ 122°F) IP8365EH: Starting Temperature: -40°C ~ 50°C (-40°F ~ 122°F) (PoE: -10°C ~ 50°C) Working Temperature: -50°C ~ 50°C (-58°F ~ 122°F)
Warranty	24 months
System Requirements	
Operating System	Microsoft Windows 8/7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~10 (streaming only) Internet Explorer 7/8/9/10
Other Players	VLC: 1.1.11 or above Quicktime: 7 or above
Included Accessories	
CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Others	Quick installation guide, warranty card, sun shield, wall mount bracket, waterproof RJ45 Ethernet enclosure, alignment sticker, desiccant bag, waterproof connector

Dimensions



Compatible Accessories

Mounting Kits

AM-311
Pole Mount Adaptor

AM-411
Corner Mount Adaptor

PoE Kits

POE-IJ-1748NDN
PoE injector, 802.3af compliant

All specifications are subject to change without notice. Copyright © VIVOTEK INC. All rights reserved.

Distributed by:

VIVOTEK
WWW.VIVOTEK.COM

Ver 1.2

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho,
New Taipei City, 235, Taiwan, R.O.C.
T: +886-2-82455282 F: +886-2-82455532
E: sales@vivotek.com

VIVOTEK USA
2050 Ringwood Avenue,
San Jose, CA 95131
T: 408-773-8686 F: 408-773-8298
E: salesusa@vivotek.com

VIVOTEK Europe
Randstad 22-133, 1316BW Almere,
The Netherlands
E: saleseurope@vivotek.com

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準にづくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.